FORM PTO-1390 US DEPARTMENT OF COMMERCE REV. 5-93 PATENT AND TRADEMARK OFFICE **TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371**	ATTORNEYS DOCKET NUMBER P99,2497 U.S.APPLICATION NO. (if known, see 37 CFR 1.5) 09/446425

INTERNATIONAL APPLICATION NO. **PCT/DE98/01693**	INTERNATIONAL FILING DATE **19 June 1998**	PRIORITY DATE CLAIMED 26 June 1997

TITLE OF INVENTION
METHOD AND APPARATUS FOR ENCODING, TRANSMITTING AND DECODING A DIGITAL MESSAGE

APPLICANT(S) FOR DO/EO/US
Christoph Capellaro et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. □ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. □ has been transmitted by the International Bureau.
   c. □ is not required, as the application was filed in the United States Receiving Office (RO/US)

6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))
   a. □ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. □ have been transmitted by the International Bureau.
   c. □ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. □ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). **EXECUTED**

10 □ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; (PTO 1449, Prior Art, Search Report)

12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. (See attached envelope)

13. ☒ A FIRST preliminary amendment.
    □ A SECOND or SUBSEQUENT preliminary amendment.

14. □ A substitute specification.

15. □ A change of power of attorney and/or address letter.

16. ☒ Other items or information:
    a. ☒ Submission of Drawings - Figs. 1-6 on eleven sheets
    b. ☒ EXPRESS MAIL #EL393830099US dated 12-20-99

U.S.APPLICATION NO. (if known, see 37 C.F.R. 1.5)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/446425	PCT/DE98/01693	P99,2497

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO . . . . $840.00 International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) . . $720.00 No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2) . . . . $790.00 Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO . . . . $1070.00 International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) . . . . $ 98.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 840.00	
Surcharge of $130.00 for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	33 - 20 =	13	X $ 18.00	$234.00	
Independent Claims	9 - 3 =	6	X $ 78.00	$468.00	
Multiple Dependent Claims			$260.00 +	$	

TOTAL OF ABOVE CALCULATIONS =	$702.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)	$	
SUBTOTAL =	$ 702.00	
Processing fee of $130.00 for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +	$	
TOTAL NATIONAL FEE =	$ 1542.00	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). $40.00 per property +		
TOTAL FEES ENCLOSED =	$ 1542.00	
	Amount to be refunded	$
	charged	$

a. ☒ A check in the amount of $ 1542.00 to cover the above fees is enclosed.

b. □ Please charge my Deposit Account No. ____________ in the amount of $ ________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 08-2290. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Hill & Simpson
A Professional Corporation
85th Floor Sears Tower
Chicago, Illinois 60606

SIGNATURE

William E. Vaughan
NAME

39,056
Registration Number

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Mailing Label Number EL393830099US

Date of Deposit: December 20, 1999

I hereby certify that this correspondence is being deposited with the United States Postal "Express Mail Post Office to Addressee" service under 37 CFR 1.10(c) on the date indicated above and is addressed to:

BOX PCT
Assistant Commissioner for Patents
Washington DC 20231

Case Number: **P99,2497**
Applicant: **Christoph Capellaro et al.**
International Application No. PCT/DE98/01693
International Filing Date 19 June 1998
Priority Date Claimed 26 June 1997
Title: METHOD AND APPARATUS FOR ENCODING, TRANSMITTING AND DECODING A DIGITAL MESSAGE

Enclosed are the following documents:
PTO 1390 in duplicate;
International application as filed; drawings
English Translation;
Information Disclosure Statement, PTO 1449, Search Report, references
Preliminary Amendment;
Submission of Drawings FIGS. 1-6 on eleven sheets
executed declaration
filing fee $1542.00
Postcard.

(See Attached envelope for executed assignment and fee)

Signature of person mailing documents and fees

BOX PCT

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

PRELIMINARY AMENDMENT

APPLICANTS: Christoph Capellaro et al. DOCKET NO: P99,2497

SERIAL NO: GROUP ART UNIT:

EXAMINER:

INTERNATIONAL APPLICATION NO: PCT/DE98/01693

INTERNATIONAL FILING DATE: 19 June 1998

INVENTION: **METHOD AND APPARATUS FOR ENCODING, TRANSMITTING AND DECODING A DIGITAL MESSAGE**

Assistant Commissioner for Patents,
Washington, D.C. 20231

Sir:

Please amend the above-identified International Application before entry into the National stage before the U.S. Patent and Trademark Office under 35 U.S.C. §371 as follows:

In The Specification:

On page 1, cancel lines 1-5 and substitute therefor:

--SPECIFICATION

TITLE

METHOD AND APPARATUS FOR ENCODING, TRANSMITTING AND DECODING A DIGITAL MESSAGE

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates, generally, to a method and apparatus for encoding, transmitting and decoding a digital message and, more specifically, to such a method and apparatus wherein cryptographic security mechanisms are provided which are simpler than those in known methods and arrangements.

Description of the Prior Art--.

On page 1, line 8, insert --both-- after “to”.

On page 1, line 9, cancel “and the” and substitute therefor --. The--.

On page 1, line 10, insert --also-- after “purpose”.

On page 1, line 11, insert --the-- after “of”.

On page 1, line 19, cancel “hitherto” and substitute therefor --the--.

On page 1, line 19, insert --protocol-- after “widespread”.

On page 1, line 20, cancel “both”.

On page 1, line 21, cancel “given” and substitute therefor --over--.

On page 1, include the paragraph which begins on line 22 in the paragraph which ends on line 21.

On page 1, line 24, cancel “as well as” and substitute therefor --and--.

On page 1, line 24, cancel “exhibits” and substitute therefor --exhibit--.

On page 1, line 25, insert a --,-- after “integrated”.

On page 1, line 26, cancel “through” and substitute therefor --or--.

On page 1, line 26, insert a --,-- after “integrated”.

On page 1, include the paragraph which begins on line 27 in the paragraph which ends on line 26.

On page 1, line 27, cancel “as well as” and substitute therefor --and--.

On page 2, line 6, cancel “are”.

On page 2, line 6, insert --are-- after “usually”.

On page 2, line 8, cancel “are”.

On page 2, line 8, insert --are-- after “also”.

On page 2, line 9, cancel "comprise" and substitute therefor --include--.

On page 2, line 11, cancel "are" and substitute therefor --is--.

On page 2, line 11, cancel "in turn".

On page 2, line 14, insert a --,-- after "as".

On page 2, line 14, insert --unit-- after "computer".

On page 2, line 16, insert --a-- before "second".

On page 2, include the paragraph which begins on line 17 in the paragraph which ends on line 16.

On page 2, line 17, cancel "is" after "computer" and substitute therefor --may be--.

On page 2, line 17, cancel "as well as " and substitute therefor --and--.

On page 2, include the paragraph which begins on line 19 in the paragraph which ends on line 18.

On page 2, line 19, cancel "realized" and substitute therefor --implemented--.

On page 2, line 19, cancel "both".

On page 2, line 21, cancel the "," and substitute therefor a --;--.

On page 2, line 21, insert a --,-- after "i.e.".

On page 2, line 22, insert --unit-- after "computer".

On page 2, line 23, cancel "computers" and substitute therefor --computer unit--.

On page 2, line 23, cancel "for".

On page 2, line 24, cancel "without further ado to".

On page 2, line 24, insert --to-- after "also".

On page 2, line 24, insert --present-- before "invention".

On page 2, line 27, cancel "units" and substitute therefor --unit,--.

On page 3, include the paragraph which begins on line 1, in the paragraph which ends on line 28 of page 2.

On page 3, line 1, insert a --,-- after “unit”.

On page 3, line 2, insert a --,-- after “protocols”.

On page 3, line 7, cancel the “,” and substitute therefor a --;--.

On page 3, line 7, insert a --,-- after “example”.

On page 3, line 8, cancel “, i.e. of” and substitute therefor a --(--.

On page 3, line 8, insert a --)-- after “unit”.

On page 3, include the paragraph which begins on line 13 in the paragraph which ends on line 12.

On page 3, include the paragraph which begins on line 15 in the paragraph which ends on line 14.

On page 3, line 18, insert --a-- before “password”.

On page 3, line 20, cancel the “,” and substitute therefor a --(--.

On page 3, line 20, insert a --,-- after “i.e.”.

On page 3, line 20, insert a --)-- after “unit”.

On page 3, line 24, cancel the “,” and substitute therefor a --;--.

On page 3, line 24, insert a --,-- after “example”.

On page 3, line 25, cancel the “,” and substitute therefor --. Such is the case--.

On page 4, line 1, insert --has-- before “no”.

On page 4, line 3, insert a --,-- after “is”.

On page 4, line 3, insert a --,-- after “thus”.

On page 4, line 4, cancel “without further ado”.

On page 4, include the paragraph which begins on line 6 in the paragraph which ends on line 5.

On page 4, line 9, insert a --,-- after “were”.

On page 4, line 10, insert a --,-- after “fact”.

On page 4, line 10, cancel “, in particular,”.

On page 4, line 11, cancel “the fact that”.

On page 4, line 11, cancel “was” and substitute therefor --being--.

On page 4, include the paragraph which begins on line 19 in the paragraph which ends on line 18.

On page 4, cancel line 22 and substitute the following centered heading therefor:

--**<u>SUMMARY OF THE INVENTION</u>**--.

On page 4, line 23, insert --present-- before “invention”.

On page 4, line 23, cancel “thus” and substitute therefor --, therefore,--.

On page 4, lines 23-24, cancel “methods as well as a computer system” and substitute therefor --a method and apparatus--.

On page 4, line 24, insert --the-- before “encoding”.

On page 4, line 25, cancel “whereby” and substitute therefor --wherein--.

On page 4, line 27, cancel “Given the method according to patent claim 1" and substitute therefor --Accordingly, in an embodiment of the present invention--.

On page 5, line 1, cancel “and” and substitute therefor --wherein--.

On page 5, line 4, insert --encoded-- before “message”.

On page 5, line 4, cancel “according to patent claim 2" and substitute therefor --described above--.

On page 5, line 4, cancel “the” after the “,” and substitute therefor --such--.

On page 5, line 7, cancel “, and the” and substitute therefor --. The--

.

On page 5, line 8, insert --then-- before “decoded”.

On page 5, line 10, cancel “Given the method according to patent claim 3" and substitute therefor --In a further embodiment of the method--.

On page 5, line 15, cancel "ensued" and substitute therefor --occurred--.

On page 5, include the paragraph which begins on line 26 in the paragraph which ends on line 25.

On page 5, lines 26-27, cancel "simple realizability and, thus, of fast implementability" and substitute therefor --being easily implemented--.

On page 5, line 28, cancel "may be seen therein" and substitute therefor --is--.

On page 6, line 2, cancel "substantially".

On page 6, line 3, insert --substantially-- after "enhanced".

On page 6, line 4, cancel "The" and substitute therefor --In an embodiment of the present invention, a--.

On page 6, line 4, cancel "according to patent claim 12".

On page 6, lines 5-6, cancel "method according to one of the claims 1 through 11 is" and substitute therefor --above-described methods are--.

On page 6, include the paragraph which begins on line 7 in the paragraph which ends on line 6.

On page 6, line 7, cancel "the" and substitute therefor --Such--.

On page 6, lines 7-8, cancel "according to patent claim 13 for encoding a digital message upon employment of an encoding format of a network protocol comprises" and substitute therefor --includes--.

On page 6, line 10, cancel "a first".

On page 6, line 12, cancel "a second".

On page 6, line 12, cancel "the cryptographic" and substitute therefor --cryptographically--.

On page 6, line 12, cancel "of".

On page 6, line 12, insert --and-- after the ";".

On page 6, line 13, cancel "a third".

On page 6, line 15, cancel "The" and substitute therefor --In an embodiment, the--.

On page 6, lines 15-16, cancel "according to patent claim 14 for decoding a digital message that is present in an encoding format of the network protocol comprises" and substitute therefor --also may include--.

On page 6, line 18, cancel "a fifth".

On page 6, line 20, cancel "a sixth".

On page 6, line 22, cancel "a seventh".

On page 6, line 22, cancel "the inverse cryptographic" and substitute therefor --inversely cryptographically--.

On page 6, line 22, cancel "of".

On page 6, line 24, cancel "an eighth".

On page 6, line 26, cancel "The" and substitute therefor --In another embodiment, the--.

On page 6, lines 26-28, cancel "according to patent claim 15 for encoding a digital message, for transmitting the message from a first computer unit to a second computer unit and for decoding the message contains" and substitute therefor --also may include--.

On page 6, line 29, cancel "comprises" and substitute therefor --includes--.

On page 7, line 1, cancel "a first".

On page 7, line 3, cancel "a second".

On page 7, line 3, cancel "the cryptographic" and substitute therefor --cryptographically--.

On page 7, line 3, cancel "of".

On page 7, line 4, cancel "a third".

On page 7, line 4, cancel "the" before "encoding".

On page 7, line 4, cancel "of".

On page 7, line 5, insert --and-- after the ";".

On page 7, line 6, cancel “a fourth”.

On page 7, line 7, insert --and-- after the “;”.

On page 7, line 8, cancel “comprises” and substitute therefor --includes--.

On page 7, line 9, cancel “a fifth”.

On page 7, line 11, cancel “a sixth”.

On page 7, line 13, cancel “a seventh”.

On page 7, line 13, cancel “the inverse cryptographic” and substitute therefor --inversely cryptographically--.

On page 7, line 13, cancel “of”.

On page 7, line 15, cancel “an eighth”.

On page 7, line 17, insert a --,-- after “systems”.

On page 7, line 17, insert a --,-- after “thus”.

On page 7, line 17, cancel “likewise”.

On page 7, line 17, insert --same type of-- before “advantages”.

On page 7, line 17, insert --as-- after “advantages”.

On page 7, line 18, cancel “method” and substitute therefor --methods of the present invention--.

On page 7, cancel lines 19-20.

On page 7, line 21, cancel “method” and substitute therefor --methods of the present invention--.

On page 7, line 21, cancel “especially”.

On page 7, line 24, cancel “this method” and substitute therefor --such methods--.

On page 7, line 25, cancel “method can” and substitute therefor --methods--.

On page 7, line 25, insert --can-- after “also”.

On page 7, line 25, cancel “the” before “other”.

On page 7, line 25, cancel the “,”.

On page 7, line 26, cancel "is".

On page 7, line 26, insert --is-- after "also".

On page 7, line 28, inset --of the present invention-- after "system".

On page 7, line 28, cancel "fashion" and substitute therefor --configure--.

On page 7, line 28, cancel "second".

On page 7, line 29, cancel "cryptographic" and substitute therefor --cryptographically--.

On page 7, line 29, cancel "of".

On page 7, line 29, cancel "third".

On page 8, line 2, cancel "fourth".

On page 8, line 4, cancel ", which" and substitute therefor --. Such proxy agent--.

On page 8, line 4, cancel "first".

On page 8, line 7, cancel "realized" and substitute therefor --embodied either--.

On page 8, line 7, cancel "can also be realized".

On page 8, line 9, cancel "realization" and substitute therefor --actualization--.

On page 8, line 14, cancel "likewise".

On page 8, line 14, cancel "fifth".

On page 8, line 15, cancel "sixth".

On page 8, line 16, cancel "of" after "decoding".

On page 8, line 17, cancel "seventh".

On page 8, line 17, cancel "the inverse cryptographic" and substitute therefor --inversely cryptographically--.

On page 8, line 17, cancel "of".

On page 8, line 18, cancel "realized" and substitute therefor --embodied--.

On page 8, cancel lines 21-24 and substitute the following therefor:

--Additional features and advantages of the present invention are described in, and will be apparent from, the Detailed Description of the Preferred Embodiments and the Drawings.

DESCRIPTION OF THE DRAWINGS--.

On page 8, line 25, insert --shows-- after "Figure 1".

On page 8, line 25, cancel "wherein" and substitute therefor --of--.

On page 8, line 25, cancel "is shown".

On page 8, line 25, cancel "realization".

On page 8, line 27, insert --shows-- after "Figure 2".

On page 8, line 27, cancel "wherein" and substitute therefor --of--.

On page 8, line 27, cancel "is shown".

On page 8, line 28, cancel "realization".

On page 8, line 29, insert --shows-- after "Figure 3".

On page 8, line 29, cancel "wherein" and substitute therefor --of--.

On page 8, line 29, cancel "is shown".

On page 9, line 1, insert --shows-- after "Figure 4".

On page 9, line 3, cancel "realized" and substitute therefor --effected--.

On page 9, line 4, insert --shows-- after "Figure 5".

On page 9, line 6, cancel "is realized" and substitute therefor --are effected--.

On page 9, line 6, insert --and-- after the ";".

On page 9, line 7, insert --shows-- after "Figure 6".

On page 9, line 9, cancel "realized" and substitute therefor --effected--.

On page 9, cancel line 10 and substitute the following centered heading therefor:

--**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**--.

On page 9, line 13, cancel “comprises” and substitute therefor --includes--.

On page 9, include the paragraph which begins on line 15 in the paragraph which ends on line 14.

On page 9, line 15, cancel “comprises” and substitute therefor --includes--.

On page 9, line 20, cancel “ensues” and substitute therefor --occurs--.

On page 9, include the paragraph which begins on line 26 in the paragraph which ends on line 25.

On page 10, include the paragraph which begins on line 1 in the paragraph which ends on line 27 of page 9.

On page 10, line 6, cancel the “,” after “method” and substitute therefor a --;--.

On page 10, line 5, insert a --,-- after “example”.

On page 10, line 6, cancel “as well”.

On page 10, line 7, cancel “as well”.

On page 10, line 7, cancel “method”.

On page 10, line 7, cancel “thereby”.

On page 10, include the paragraph which begins on line 9 in the paragraph which ends on line 8.

On page 10, line 15, cancel the “,” after “request” and substitute therefor a --;--.

On page 10, line 15, insert a --,-- after “i.e.”.

On page 10, line 20, cancel “advantageous since” and substitute therefor --so because--.

On page 10, line 26, cancel the “,” and substitute therefor a --;--.

On page 10, line 26, insert a --,-- after “i.e.”.

On page 11, line 3, cancel the "-" after "response" and substitute therefor a --,--.

On page 11, line 3, cancel the "-" after "standards" and substitute therefor a --,--.

On page 11, line 5, insert --a-- before "reply".

On page 11, line 8, cancel "i.e." and substitute therefor --or--.

On page 11, line 24, cancel the "," after "message" and substitute therefor a --;--.

On page 11, line 24, insert a --,-- after "i.e.".

On page 11, line 27, cancel "particular" and substitute therefor --particulars--.

On page 11, line 27, insert a --,-- after "is" and before "in".

On page 11, line 27, insert a --,-- after "fact".

On page 12, line 6, insert --a-- before "reply".

On page 12, line 10, insert --either-- before "can".

On page 12, line 10, cancel "either".

On page 12, line 29, cancel the "," and substitute therefor a --;--.

On page 13, line 1, insert a --,-- after "i.e.".

On page 13, line 13, cancel the "," and substitute therefor a --;--.

On page 13, line 13, insert a --,-- after "i.e.".

On page 13, line 20, cancel "i.e." and substitute therefor --or--.

On page 13, line 24, cancel "contained in the get response".

On page 14, line 4, cancel "**Net**" and substitute therefor -- **Next--.**

On page 14, line 7, cancel the "," after "modified" and substitute therefor --and--.

On page 14, line 12, cancel "fashioned" and substitute therefor --arranged--.

On page 15, line 5, cancel the "," after "decoded" and substitute therefor a --;--.

On page 15, line 5, insert a --,-- after “i.e.”.

On page 15, line 22, cancel “as well as” and substitute therefor --and--.

On page 15, line 23, insert --respectively-- before “correspond”.

On page 15, line 23, cancel “as well as to” and substitute therefor --and--.

On page 16, line 1, insert --contain-- after “can”.

On page 16, line 2, cancel “contain”.

On page 17, line 9, insert --a-- before “bit”.

On page 17, line 13, cancel the “,” and substitute therefor a --;--.

On page 17, line 15, cancel “The” and substitute therefor --Thus, the--.

On page 17, line 15, cancel “thus”.

On page 17, line 16, insert --a-- after “as”.

On page 17, line 18, cancel “then,”.

On page 17, line 19, cancel the “,” and substitute therefor a --;--.

On page 17, line 19, insert a --,-- after “i.e.”.

On page 18, line 2, cancel “example” and substitute therefor --instance--.

On page 18, line 2, cancel the “,” after “303" and substitute therefor a --;--.

On page 18, line 2, insert a --,-- after “example”.

On page 18, line 22, cancel the “,” and substitute therefor a -- - --.

On page 18, line 25, insert a --,-- after “can”.

On page 18, line 25, insert a --,-- after ‘thereby”.

On page 18, line 28, cancel the “,” and substitute therefor a --;--.

On page 18, line 28, insert a --,-- after “example”.

On page 19, line 1, cancel “The realization” and substitute therefor --Further--.

On page 19, line 9, cancel “, as” and substitute therefor --. As--.

On page 19, line 9, insert a --,-- after “result”.

On page 19, line 9, cancel “whereof”.

On page 19, line 21, cancel “comprising” and substitute therefor --including--.

On page 19, line 23, cancel the “,” and substitute therefor a --;--.

On page 19, line 24, cancel the “,” and substitute therefor a --;--.

On page 19, line 25, cancel the “,” and substitute therefor --; or--.

On page 20, line 3, cancel “comprise” and substitute therefor --include--.

On page 20, line 4, cancel the “,” and substitute therefor a --;--.

On page 20, line 5, cancel the “,” and substitute therefor a --;--.

On page 20, line 6, cancel the “,” and substitute therefor --; or--.

On page 20, line 17, cancel “comprises” and substitute therefor a --includes--.

On page 20, line 22, cancel “ensue” and substitute therefor --occur--.

On page 20, line 24, cancel “can”.

On page 20, line 24, insert --can-- after “again”.

On page 21, line 3, cancel “very advantageously”.

On page 21, line 4, insert --quite advantageously-- after “employed”.

On page 21, line 7, insert --both-- before “the method”.

On page 21, line 7, cancel “as well as” and substitute therefor --and-- .

On page 21, line 8, cancel “advantageously”.

On page 21, line 8, cancel “for controlling” and substitute therefor --to control--.

On page 21, lines 8-9, cancel “for accounting” and substitute therefor --to account--.

On page 21, line 10, cancel “realized” and substitute therefor --located--.

On page 21, line 11, cancel “realized” and substitute therefor --located--.

On page 21, line 21, cancel “as well” and substitute therefor --and--.

On page 21, line 26, cancel “as well, a” and substitute therefor --. A--.

On page 21, line 28, cancel “being” and substitute therefor --is--.

On page 22, after line 3, insert the following paragraph:

--Although the present invention has been described with reference to specific embodiments, those of skill in the art will recognize that changes may be made thereto without departing from the spirit and scope of the invention as set forth in the hereafter appended claims.--

On page 31 (last page), cancel line 1 and substitute the following centered heading therefor:

--**<u>ABSTRACT OF THE DISCLOSURE</u>**--.

On page 31, line 5, cancel “is presented” and substitute therefor --and apparatus--.

On page 31, lines 5-6, cancel “, for example for the SNMPv1,”.

On page 31, line 6, cancel “(101)”.

On page 31, line 6, cancel “the” and substitute therefor --a--.

On page 31, line 6, cancel “(C1)”.

On page 31, line 8, cancel “(CN)”.

On page 31, line 8, cancel “(CN)”.

On page 31, line 8, cancel “(104)”.

On page 31, line 9, cancel “(KBN)”.

On page 31, line 10, cancel “(105)”.

On page 31, line 11, cancel “(CKN)”.

On page 31, line 12, cancel “(C1)”.

On page 21, line 12, cancel "(C2)".

On page 31, line 13, cancel "(C2)".

On page 31, line 13, cancel "(109)".

On page 31, line 15, cancel "(110)".

On page 31, line 15, cancel "(DKN)".

On page 31, line 16, cancel "(IKN)".

On page 31, cancel line 18.

In the Claims:

On page 23, cancel line 1 and substitute the following left-hand justified heading therefor:

--**We Claim As Our Invention**--.

Please cancel claims 1-27, without prejudice, and substitute the following claims therefor:

28. A method for encoding a digital message, the method comprising the steps of:

encoding the digital message to form an encoded message upon employment of an encoding format of a network protocol;

subjecting the encoded message to at least one cryptographic process to form a cryptographically processed message; and

encoding the cryptographically processed message upon employment of the encoding format of the network protocol.

29. A method for decoding an encoded, cryptographically processed message that is present in an encoding format of a network protocol, the method comprising the steps of:

decoding the encoded, cryptographically processed message according to the encoding format of the network protocol to form a decoded, cryptographically processed message;

subjecting the decoded, cryptographically processed message to a second cryptographic process inverse relative to an at least one first cryptographic process, which previously encoded an original digital message, to form an inversely cryptographically processed message; and

decoding the inversely cryptographically processed message according to the encoding format of the network protocol.

30. A method for encoding a digital message, for transmitting the digital message from a first computer unit to a second computer unit and for decoding the digital message, the method comprising the steps of:

encoding the digital message, in the first computer unit, to form an encoded message upon employment of an encoding format of a network protocol;

subjecting the encoded message, in the first computer unit, to at least one first cryptographic process to form a crypto graphically processed message;

encoding the cryptographically processed message, in the first computer unit, upon employment of the encoding format of the network protocol to form an encoded, cryptographically processed message;

transmitting the encoded, cryptographically processed message from the first computer unit to the second computer unit;

decoding the encoded, cryptographically processed message, in the second computer unit, according to the encoding format of the network protocol to form a decoded, cryptographically processed message;

subjecting the decoded, cryptographically processed message, in the second computer unit, to a second cryptographic process inverse relative to the at least one first cryptographic process to form an inversely cryptographically processed message; and decoding the inversely cryptographically processed message, in the second computer unit, into the digital message according to the encoding format of the network protocol.

31. A method for encoding a digital message, for transmitting the digital message from a first computer unit to a second computer unit and for decoding the digital message as claimed in claim 30, further comprising the steps of:

including a request for implementing a prescribable action in the digital message;

implementing the prescribable action in the second computer unit to obtain a result of the prescribable action; and

sending the result of the prescribable action from the second computer unit to the first computer unit in a reply message.

32. A method for encoding a digital message, for transmitting the digital message from a first computer unit to a second computer unit and for decoding the digital message as claimed in claim 30, further comprising the steps of:

including a request for implementing a prescribable action in the digital message;

implementing the prescribable action in the second computer unit to obtain a result of the prescribable action;

forming a reply message which contains the result of the prescribable action in the second computer unit;

encoding the reply message in the second computer unit according to the encoding format of the network protocol to form an encoded reply message;

subjecting the encoded reply message to at least one cryptographic process in the second computer unit to form a cryptographically processed reply message;

storing the cryptographically processed reply message in the second computer unit;

encoding a fetch message in the first computer unit according to the encoding format of the network protocol, wherein the cryptographically processed reply message is requested from the second computer unit with the fetch message;

transmitting the fetch message from the first computer unit to the second computer unit;

receiving the fetch message by the second computer unit;

encoding the cryptographically processed reply message according to the encoding format of the network protocol to form an encoded, crypto graphically processed reply message; and

transmitting the encoded, cryptographically processed reply message from the second compute unit to the first computer unit.

33. A method for encoding a digital message, for transmitting the digital message from a first computer unit to a second computer unit and for decoding the digital message as claimed in claim 30, the method further comprising the steps of:

including a request for implementing a prescribable action in the digital message;

implementing the prescribable action in the second computer unit to obtain a result of the prescribable action;

forming a reply message which contains the result of the prescribable action in the second computer unit;

encoding the reply message in the second computer unit according to the encoding format of the network protocol to form an encoded reply message;

subjecting the encoded reply message to at least one cryptographic process in the second computer unit to form a cryptographically processed reply message;

encoding the cryptographically processed reply message according to the encoding format of the network protocol to form an encoded, crypto graphically processed reply message; and

transmitting the encoded, cryptographically processed reply message from the second computer unit to the first computer unit.

34. A method for encoding a digital message, for transmitting the digital message from a first computer unit to a second computer unit and for decoding the digital message as claimed in claim 33, wherein the cryptographically processed reply message is stored in a management information base in the second computer unit.

35. A method for encoding a digital message as claimed in claim 28, wherein the network protocol is a simple network management protocol version 1.

36. A method for encoding a digital message as claimed in claim 35, further comprising the steps of:

forming a set request in the first computer unit upon encoding the cryptographically processed message; and

transmitting the set request from the first computer unit to the second computer unit.

37. A method for encoding a digital message, for transmitting the digital message from a first computer unit to a second computer unit and for decoding the digital message as claimed in claim 32, further comprising the steps of:

employing a get request as the fetch message; and

forming a get response upon the encoding of the requested, cryptographically processed reply message.

38. A method for encoding a digital message, for transmitting the digital message from a first computer unit to a second computer unit and for decoding the digital message as claimed in claim 31, further comprising the step of:

transmitting as the prescribable action at least one of an information query and an information indication of the second computer unit.

39. An apparatus for encoding a digital message, the apparatus comprising:

means for encoding the digital message upon employment of an encoding format of a network protocol to form an encoded message;

means for cryptographically processing the encoded message to form a cryptographically processed message; and

means for encoding the cryptographically processed message upon employment of the encoding format of the network protocol.

40. An apparatus for decoding an encoded, cryptographically processed message that is present in an encoding format of a network protocol, the apparatus comprising:

means for receiving the encoded, cryptographically processed message from a first computer unit;

means for decoding the encoded, cryptographically processed message according to the encoding format of the network protocol to form a decoded, cryptographically processed message;

means for inversely cryptographically processing the decoded, cryptographically processed message to form an inversely cryptographically processed message; and

means for decoding the inversely cryptographically processed message according to the encoding format of the network protocol.

41. An apparatus for encoding, transmitting and decoding a digital message, comprising:

a first computer unit, the first computer unit including means for encoding the digital message upon employment of an encoding format of a network protocol to form an encoded message, means for cryptographically processing the encoded message to form a cryptographically processed message, means for encoding the cryptographically processed message upon employment of the encoding format of the network protocol to form an encoded, cryptographically processed message, and means for sending the encoded cryptographically processed message from the first computer unit to the second computer unit; and

a second computer unit, the second computer unit including means for receiving the encoded cryptographically processed message from the first computer unit, means for decoding the encoded cryptographically processed message according to the encoding format of the network protocol to form a decoded cryptographically processed message, means for inversely cryptographically processing the decoded cryptographically processed message to form an inversely cryptographically processed message, and means for decoding the inversely cryptographically processed message according to the encoding format of the network protocol.;

42. An apparatus for encoding a digital message as claimed in claim 39, wherein the means for encoding the digital message is further provided as the means for encoding the cryptographically processed message.

43. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 41, wherein the means for encoding the digital message is further provided as the means for encoding the cryptographically processed message.

44. An apparatus for decoding an encoded, cryptographically processed message that is present in an encoding format of a network protocol as claimed in claim 40, wherein the means for decoding the encoded, cryptographically processed message is further provided as the means for decoding the inversely cryptographically processed message.

45. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 41, wherein the means for decoding the encoded, cryptographically processed message is further provided as the means for decoding the inversely cryptographically processed message.

46. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 41, wherein the digital message contains a request for implementing a prescribable action, the apparatus further comprising:

means for implementing the prescribable action to obtain a result of the prescribable action, the means for implementing being provided in the second computer unit; and means for sending the result of the prescribable action to the first computer unit, the means for sending being provided in the second computer unit.

47. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 41, wherein the digital message contains a request for implementing a prescribable action, the apparatus further comprising:

means for implementing the prescribable action to obtain a result, the means for implementing being provided in the second computer unit;

means for forming a reply message that contains the result of the prescribable action, the means for forming a reply message being provided in the second computer unit;

means for encoding the reply message according to the encoding format of the network protocol to form an encoded reply message, the means for encoding the reply message being provided in the second computer unit;

means for processing the encoded reply message with at least one cryptographic process to form a cryptographically processed encoded reply message, the means for processing the encoded reply message being provided in the second computer unit;

means for storing the cryptographically processed encoded reply message, the means for storing being provided in the second computer unit;

means for forming and encoding a fetch message according to the encoding format of the network protocol wherein the cryptographically processed encoded reply message is requested from the second computer unit, the means for forming and encoding a fetch message being provided in the first computer unit;

means for sending the fetch message from the first computer unit to the second computer unit, the means for sending the fetch message being provided in the first computer unit;

means for receiving the fetch message, the means for receiving the fetch message being provided in the second computer unit;

means for encoding the cryptographically processed reply message requested in the fetch message according to the encoding format of the network protocol, the means for encoding the cryptographically processed reply message being provided in the second computer unit; and

means for sending the encoded, cryptographically processed reply message from the second computer unit to the first computer unit, the means for sending the encoded, cryptographically processed reply message being provided in the second computer unit.

48. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 41, wherein the digital message contains a request for implementing a prescribable action, the apparatus further comprising:

means for implementing the prescribable action to obtain a result of the prescribable action, the means for implementing the prescribable action being provided in the second computer unit;

means for forming a reply message that contains the result of the prescribable action, the means for forming the reply message being provided in the second computer unit;

means for encoding the reply message according to the encoding format of the network protocol to form an encoded reply message, the means for encoding the reply message being provided in the second computer unit;

means for processing the encoded reply message with at least one cryptographic process to form a cryptographically processed encoded reply message, the means for processing the encoded reply message being provided in the second computer unit;

means for encoding the cryptographically processed encoded reply message according to the encoding format of the network protocol to form an encoded, cryptographically processed encoded reply message, the means for encoding the cryptographically processed encoded reply message being provided in the second computer unit; and

means for sending the encoded, cryptographically processed encoded reply message from the second computer unit to the first computer unit, the means for sending the encoded, cryptographically processed encoded reply message being provided in the second computer unit.

49. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 47, wherein the cryptographically processed reply message is stored in a management information base.

50. An apparatus for encoding a digital message as claimed in claim 39, wherein the network protocol is a simple network management protocol version 1.

51. An apparatus for decoding an encoded, cryptographically processed message that is present in an encoding format of a network protocol as claimed in claim 40, wherein the network protocol is the simple network management protocol version 1.

52. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 41, wherein the network protocol is a simple network management protocol version 1.

53. An apparatus for encoding a digital message as claimed in claim 39, wherein the network protocol is a simple network management protocol version 1, and wherein the means for encoding the cryptographically processed message is configured such that a set request is formed upon the encoding of the cryptographically processed message.

54. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 41, wherein the network protocol is a simple network management protocol version 1, and wherein the means for encoding the cryptographically processed message is configured such that a set request is formed upon the encoding of the cryptographically processed message.

55. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 47, wherein the means for forming and encoding the fetch message is configured such that a get request is formed, and wherein the means for encoding the cryptographically processed reply message requested in the fetch message is configured such that a get response is formed.

56. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 41, wherein at least one of an information query and an information particular of the computer unit is provided as the prescribable action.

57. An apparatus for encoding, transmitting and decoding a digital message as claimed in claim 56, wherein the means for cryptographically processing the encoded message, the means for encoding the cryptographically processed message and the means for sending the encoded cryptographically processed message are formed together as a first proxy agent, and wherein the means for receiving the encoded cryptographically processed message, the means for decoding the encoded cryptographically processed message and the means for inversely cryptographically processing the decoded crypto graphically processed message are formed together as a second proxy agent.

58. A communication system having a manager of a communication network and an intermediate manager of a communication network, the communication system employing the communication network and offering further services that proceed beyond services offered by the communication network to customers, the communication system including an apparatus for encoding a digital message which comprises:

means for encoding the digital message upon employment of an encoding format of a network protocol to form an encoded message;

means for cryptographically processing the encoded message to form a cryptographically processed message; and

means for encoding the cryptographically processed message upon employment of the encoding format of the network protocol.

59. A communication system having a manager of a communication network and an intermediate manager of a communication network, the communication system employing the communication network and offering further services that proceed beyond services offered by the communication network to customers, the communication system including

an apparatus for decoding an encoded, cryptographically processed message that is present in an encoding format of a network protocol, the apparatus comprising:

means for receiving the encoded, cryptographically processed message from a first computer unit;

means for decoding the encoded, cryptographically processed message according to the encoding format of the network protocol to form a decoded, cryptographically processed message;

means for inversely cryptographically processing the decoded, cryptographically processed message to form an inversely cryptographically processed message; and

means for decoding the inversely cryptographically processed message according to the encoding format of the network protocol.

60. A communication system having a manager of a communication network and an intermediate manager of a communication network, the communication system employing the communication network and offering further services that proceed beyond services offered by the communication network to customers, the communication system including an apparatus for encoding, transmitting and decoding a digital message, the apparatus comprising:

a first computer unit, the first computer unit including means for encoding the digital message upon employment of an encoding format of a network protocol to form an encoded message, means for cryptographically processing the encoded message to form a cryptographically processed message, means for encoding the cryptographically processed message upon employment of the encoding format of the network protocol to form an encoded, cryptographically processed message, and means for sending the encoded cryptographically processed message from the first computer unit to the second computer unit; and

a second computer unit, the second computer unit including means for receiving the encoded cryptographically processed message from the first computer unit, means for decoding the encoded cryptographically processed message according to the encoding format of the network protocol to form a decoded cryptographically processed message, means for inversely cryptographically processing the decoded cryptographically processed message to form an inversely cryptographically processed message, and means for decoding the inversely cryptographically processed message according to the encoding format of the network protocol.

REMARKS

The present amendment makes editorial changes and corrects typographical errors in the specification in order to conform the specification to the requirements of the United States Patent practice. No new matter is added thereby. Original claims 1-27 have been canceled in favor of new claims 28-60. However, claims 28-60 have been presented solely because the revisions by bracketing and underlining which would have been necessary in claims 1-27 in order to conform those claims to the requirements of United States Patent practice would have been too extensive, and thus would have been too burdensome. The cancellation of claims 1-27 does not constitute an intent on the part of the Applicant to surrender any of the subject matter of claims 1-27.

Early consideration on the merits is respectfully requested.

Respectfully submitted,

(Reg.No. 39,056)

William E. Vaughan
Hill & Simpson
A Professional Corporation
85th Floor Sears Tower
Chicago, Illinois 60606
(312) 876-0200
Attorneys for Applicants

1. TITLE

Method and Computer System for Encoding a digital message, for transmission of the message from a first computer unit to a second computer unit, and for decoding the message

2. Technological Background

Various network protocols are known in the area of managing computer networks. The jobs for the management of computer networks are becoming increasingly more difficult due to the great spread of computers and the more and more complex networking of computers and the systems for network management required for this purpose are becoming more and more powerful. The question of security of the network management is acquiring greater and greater significance in the framework of management of computer networks. The security of the network management is highly dependent on the security techniques employed in the system.

The document (M. Rose, The Simple Book, PTR Prentice Hall, 2nd Edition, ISBN 0-13-177254-6, pages 59-91, 1994) discloses various network protocols for network management, for example the Simple Network Management Protocol (SNMP) in Version 1 (SNMPv1) and in Version 2 (SNMPv2) or the Common Management Internet Protocol (CMIP) as well.

The SNMPv1 has been hitherto most widespread for monitoring and supervision of network components both over local computer networks (Local Area Networks, LANs) as well as given global networks (Wide Area Networks, WANs).

The SNMPv1 is arranged above the Internet protocols of user datagram protocol (UDP) and Internet protocol (IP) in the framework of the OSI Communication Layer system. Both the UDP as well as the IP exhibits substantial weaknesses in the area of security, since security mechanisms are hardly integrated through not at all integrated in these protocols.

Below, both the SNMP as well as CMIP are referred to as network protocol.

The network protocols are employed for the transmission of computer network management information between a first computer unit, which contains what is referred to as a manager, and at least one second computer unit, which contains what is referred to as an agent. In a complex computer network, at least one management station and an arbitrary plurality of computers monitored and supervised by the manager application are usually monitored or, respectively, controlled via the network protocol.

However, network management architectures are also known that comprise a plurality of hierarchies, for example a plurality of computers that are respectively monitored by one manager, and a plurality of computers that respectively contain a manager application that are monitored or, respectively, controlled in turn by a further computer that contains a higher-ranking manager application.
A computer that contains a manager application of the respective network protocol is referred to below as first computer.

Each computer unit that has an agent implemented is referred to below as second computer unit.

It is possible that a computer is configured both as manager as well as as agent; correspondingly, the functionalities are contained in the computer.

The respective network protocol can be realized in the computer both in hardware as well as in software.

A simple hierarchy is assumed below, i.e. only that case is described wherein a first computer as manager monitors or, respectively, controls an arbitrary plurality of second computers, the agents. This, however, only serves for the purpose of a simpler presentation. It is possible without further ado to also apply the invention in an architecture having an arbitrary plurality of hierarchy levels.

In the network protocols, either an information query is transmitted from the first computer unit to the second computer units or a control value is transmitted for the control or, respectively, supervision of the second computer unit.

It is standard in each second computer unit given the known network protocols that the information employed by the second computer unit in the framework of the network protocol is stored in the form of what is rèferred to as a management information base (MIB), which exhibits the structure of a hierarchic data bank.

The overall structure of the management information of the network protocols is stored in what is referred to as a global registration tree, for example the global SNMP registration tree. The MIB of an agent, i.e. of a second computer unit, is a part of the registration tree of the respective network protocol.

Digital messages, for example an SNMPv1 message, are employed for the transmission of information between the first computer unit and the second computer unit.

An SNMPv1 message contains a version number, what is referred to as a community string, and an SNMPv1 protocol data unit (PDU).

The version of the network protocol employed is indicated with the version number. The version number is defined upon implementation of the respective network protocol.

The community string in the SNMPv1 serves as password for access to an MIB of a second computer unit. The community string given SNMPv1 is sent to the agent unencrypted. A check is carried out in the agent, i.e. the second computer unit, to see whether the community string that was respectively received together with an SNMPv1 message authorizes an access in the MIB of the second computer. Since the password is transmitted unencrypted given SNMPv1, a misuse of the community string is easily possible, for example for masking a potential attacker and for unauthorized access to a second computer unit, since it is very simple for a potential attacker to tap the community string together with an IP sender address of an authorized user.

SNMPv1 thus has practically no effective security mechanism integrated in it, particularly no effective authentification of the SNMPv1 manager, and, as a consequence of the lacking authentification, no dependable access control on the part of the agent. Further, SNMPv1 contains no possibility for implementing security mechanisms of the data integrity or of the data confidentiality. It is thus possible without further ado for a potential attacker to simply listen in to transmitted SNMP-PDUs and to misuse the transmitted information between manager and agent.

The encoding rules of the network protocols are described in detail in M. Rose, The Simple Book, PTR Prentice Hall, 2nd Edition, ISBM 0-13-177254-6, pages 59-91, 1994.

In the second version of SNMP, SNMPv2, various security measures were in fact provided but, in particular, the administration of cryptographic keys was so involved that this problem led to the fact that the SNMPv2 was incapable of prevailing in the marketplace over the SNMPv1 despite considerably greater possibilities for the administration of computer networks compared to SNMPv1. The original SNMPv2 standard was therefore withdrawn and replaced by a modified standard wherein no security was integrated.

CMIP, which due to generally significantly greater complexity compared to SNMPv1 and SNMPv2, was hardly considered in products was incapable of prevailing in the marketplace.

Further, the concept of what is referred to as proxy agents is likewise described in the document of (M. Rose, The Simple Book, PTR Prentice Hall, 2nd Edition, ISBN 0-13-177254-6, page 315, 1994).

3. Brief Description of the Invention

The invention is thus based on the problem of specifying methods as well as a computer system for encoding, transmission and decoding of a digital message, whereby cryptographic security mechanisms are provided that are simpler than in the known methods and arrangements.

Given the method according to patent claim 1, a digital message that is to be transmitted from the first computer unit to the second computer unit is encoded into an encoded message upon employment of an encoding format of a network protocol. The encoded message is subjected to at least one cryptographic process and the cryptographically processed, encoded message is again encoded upon employment of the encoding format of the network protocol.

Given the message according to patent claim 2, the message is decoded according to the encoding format of the network protocol. Further, the decoded, cryptographically processed message is subjected to a cryptographic method inverse relative to the at least one cryptographic method, and the inversely cryptographically processed message is decoded according to the encoding format of the network protocol.

Given the method according to patent claim 3, a digital message that is to be transmitted from the first computer unit to the second computer unit is encoded into an encoded message upon employment of an encoding format of a network protocol. The encoded message is subjected to at least one cryptographic process and the cryptographically processed, encoded message is again encoded upon employment of the encoding format of the network protocol. After the encoding has ensued, the entire message is transmitted from the first computer unit to at least the second computer unit. The received message is decoded in the second computer unit according to the encoding format of the network protocol. Subsequently, the decoded message is subjected to the cryptographic process inverse relative to the cryptographic process employed. In a last step, the inversely cryptographically processed message is decoded according to the encoding format of the network protocol.

As a result of the "double" encoding or, respectively, decoding with the respective network protocol, a very simple solution conforming to the standards is proposed in order to cryptographically secure the transmission of messages of a network protocol.

The method also exhibits the considerable advantage of simple realizability and, thus, of fast implementability with the assistance of a computer. A further advantage may be seen therein that the network protocols can remain unmodified and no new network protocols need be defined. Thus, no complicated version switching or even redefinition of network protocols is required. The cryptographic security of the respective network protocol can be substantially enhanced without greater outlay.

The computer system according to patent claim 12 contains at least one computer unit that is configured such that the method according to one of the claims 1 through 11 is implemented.

The computer system according to patent claim 13 for encoding a digital message upon employment of an encoding format of a network protocol comprises at least the following components:

- a first means for encoding the digital message upon employment of the encoding format of the network protocol to form an encoded message;
- a second means for the cryptographic processing of the encoded message;
- a third means for encoding the cryptographically processed message upon employment of the encoding format of the network protocol.

The computer system according to patent claim 14 for decoding a digital message that is present in an encoding format of the network protocol comprises at least the following components:

-- a fifth means for receiving the encoded, cryptographically processed message from the first computer unit;

-- a sixth means for decoding the received message according to the encoding format of the network protocol;

-- a seventh means for the inverse cryptographic processing of the decoded, cryptographically processed message; and

-- an eighth means for decoding the inversely cryptographically processed message according to the encoding format of the network protocol.

The computer system according to patent claim 15 for encoding a digital message, for transmitting the message from a first computer unit to a second computer unit and for decoding the message contains at least the following components:

- a first computer unit that comprises at least the following components:

-- a first means for encoding the digital message upon employment of an encoding format of a network protocol to form an encoded message;

-- a second means for the cryptographic processing of the encoded message;

-- a third means for the encoding of the cryptographically processed message upon employment of the encoding format of the network protocol;

-- a fourth means for sending the encoded, cryptographically processed message from the first computer unit to the second computer unit;

- a second computer unit that comprises at least the following components:

-- a fifth means for receiving the encoded cryptographically processed message from the first computer unit;

-- a sixth means for decoding the received message according to the encoding format of the network protocol;

-- a seventh means for the inverse cryptographic processing of the decoded, cryptographically processed message; and

-- an eighth means for decoding the inversely cryptographically processed message according to the encoding format of the network protocol.

The computer systems thus likewise exhibit the advantages described above in conjunction with the method.

Advantageous developments of the invention derive from the dependent claims.

The method can be especially advantageously employed in conjunction with SNMPv1 as network protocol, since practically no cryptographic security was previously present for SNMPv1.

However, this method and the corresponding arrangement for the implementation of the method can also be employed in the other network protocols, since the overall complexity of the respective network protocol therein is also considerably reduced.

Further, it is advantageous in the computer system to fashion a second means for cryptographic processing of the encoded message, a third means for encoding the cryptographically processed message upon employment of the encoding format of the network protocol as well as a fourth means for sending the encoded, cryptographically processed message to the second computer unit as what is referred to as a proxy agent, which is connected to the first means for encoding the digital message upon employment of the network protocol via a communication connection that is assumed to be secure. The first proxy agent and the first computer unit can be realized in common in one computer unit or can also be realized in two different computer units.

In this way, the realization of a computer system for cryptographically secure transmission of messages of the encoding format of a network protocol is achieved upon employment of the proxy technique, which is known from the document of (M. Rose, The Simple Book, PTR Prentice Hall, 2nd Edition, ISBN 0-13-177254-6, page 315, 1994).

This advantage can likewise be established when a fifth means for the reception of the encoded, cryptographically processed message, a sixth means for the decoding of the received message according to the encoding format of the network protocol as well as a seventh means for the inverse cryptographic processing of the decoded cryptographically processed message are realized together in a second proxy agent that is connected to the agent of the second computer unit upon employment of the network protocol via a communication connection assumed to be secure.

4. Brief Description of the Figures

The figures show an exemplary embodiment of the invention, which is explained in greater detail below.

Shown are:

Figure 1 a flowchart wherein the inventive method is shown with realization details for a get request;

Figure 2 a flowchart wherein the method is shown in terms of its method steps with realization details for a set request;

Figure 3 a flowchart wherein the method is shown in abstract form;

Figure 4 a schematic illustration of a possible structure of a cryptographically processed SNMPv1 message wherein the security mechanism of authentification of the original data is realized;

Figure 5 the structure of a possible, cryptographically processed SNMPv1 message with which the security services of integrity and confidentiality of the transmitted SNMPv1 message is realized;

Figure 6 the possible structure of a cryptographically processed SNMPv1 message wherein the security service of confidentiality of the SNMPv1 message is realized.

5. Figure Description

Get-Request

Figure 1 symbolically shows a first computer unit C1 and a second computer unit C2. The first computer unit C1 comprises a manager application MA of the SNMPv1 as well as a first proxy agent PA1.

The second computer unit C2 comprises an SNMPv1 agent AG as well as a second proxy agent PA2 at the side of the second compute C2.

In a first step 101, a get request is formed in the first computer unit C1. What is to be understood by formation of a get request is that a digital message is encoded upon employment of an encoding format of the SNMPv1 network protocol to form an encoded message, the get request. This ensues in a first means 101 of the first computer unit C1 for encoding the digital message upon employment of the encoding format of the network protocol.

In a second step 102, the get request, i.e. the encoded message CN, is sent from the first means M1 to the first proxy agent P1 at the side of the first computer unit C1.

In a third step 103, the encoded message CN is received in the first proxy agent PA1.

In a fourth step 104, the encoded message CN is subjected to at least one cryptographic process in the first proxy agent PA1. A second means 104 is utilized for the cryptographic processing of the encoded message in the fourth step 104.

What is to be understood by a cryptographic method is any arbitrary cryptographic method, for example for authentification, for securing the data integrity or for encryption of digital data as well. For example, the RSA method or the data encryption standard as well, which is referred to as DES method, can thereby be employed.

As a result, one obtains a cryptographically processed message KBN whose format is shown, for example, in Figures 3 through 6 and explained in greater detail below.

In a fifth step 105, the cryptographically processed message KBN is again encoded upon employment of the encoding format of the SNMP network protocol. What is to be understood by this method step is that the cryptographically processed get request is preferably encoded in a set request, i.e. encapsulated. Further, a third means 105 for the encoding of the cryptographically processed message upon employment of the encoding format of the network protocol is provided.

As becomes clear below, it is advantageous to encode any type of message that is to be transmitted from the first computer unit C1 to the second computer unit C2 as set request in the fifth step 105. This is advantageous since the syntax of SNMPv1 only allows object identifiers as payload data to be transmitted for a get request. It is not possible in SNMPv1 to involve the cryptographically processed information in an SNMP get request.

In a sixth step 106, the set request is transmitted as encoded, cryptographically processed message CKN from the first computer unit C1 to the second computer unit C2, i.e. from the first proxy agent PA1 to a second proxy agent PA2.

The encoded, cryptographically processed message CKN is received in a seventh step 107 by the second proxy agent PA2 of the second computer unit C2. To this end, a fifth means 107 is provided for the reception of the encoded, cryptographically processed message CKN.

In an eighth step 108, a get response - in conformity with standards - is sent from the second proxy agent PA2 to the first proxy agent PA1 of the first computer unit C1 as reply to the set request. The get response contains the respective error status as confirmation.

In a ninth step 109, the received, encoded, cryptographically processed message CKN is de-encapsulated, i.e. decoded, upon employment of the encoding format of the network protocol. A sixth means 109 is provided for the decoding of the received message corresponding to the encoding format of the SNMPv1 protocol.

In a tenth step 110, the second proxy agent PA2 applies the cryptographic process inverse relative to the respectively provided cryptographic process, for example for authentification, for decryption or, respectively, for securing the integrity of the transmitted data, onto the decoded, cryptographically processed message DKN. A seventh means 110 for the inverse cryptographic processing of the decoded, cryptographically processed message DKN is provided for this purpose.

Further, the inversely cryptographically processed message IKN, i.e. the original get request, is sent from the second proxy agent PA2 to the agent application AG of the second computer unit C2.

In an eleventh step 111, the get request is received by the agent AG. An eighth means 111 for reception of the get request is provided for this purpose.

In a further step 112, the inversely cryptographically processed message is decoded according to the encoding format of the SNMPv1 protocol to form the digital message, i.e. is interpreted. This means that, for the specific instant of the get request, the information requested via the get request, namely of a value of what is referred to as a managed object (MO) that is stored in the MIB of the agent AG, is read out. The particular as to what information is in fact requested is contained in the original get request as object identifier.

The requested action, the read out of the requested information in this case, a value of a managed object, is thus implemented in the twelfth step 112. To this end, a ninth means 112 is provided for the implementation of the requested action.

As provided in SNMPv1, a get response is formed by the agent AG in the second computer unit as reply to a get request and, in a thirteenth step 113, is sent to the second proxy agent PA2. The get response contains the result of the action that was requested by the first computer unit C1 in the get request.

The get response is referred to below as reply message AN. The reply message AN can be transmitted either directly to the first computer unit C1 or, for further enhancement of the cryptographic security, can be encoded again in conformity with the encoding format of the network protocol. A tenth means 112 for sending the result of the action to the first computer unit C1 is provided in the second computer unit C2.

Further, an eleventh means 113 is provided for forming the reply message AN that contains the result of the action and for encoding the reply message AN according to the encoding format of the SNMPv1 protocol.

In a fourteenth method step 114, the second proxy agent PA2 receives the reply message AN. A twelfth means 114 for the reception of the reply message AN is provided for this purpose.

In a fifteenth step 115, the encoded reply message AN is subjected to at least one cryptographic process. For this purpose, a thirteenth means 115 is provided for processing the reply message AN with at least one cryptographic process. The result of this method step is a get response encapsulated in a security frame.

The cryptographically processed reply message KBAN is stored in a security MIB in the second processing agent PA2 (step 116). The structure of the security MIB is described in greater detail later.

In order to obtain to the cryptographically processed reply message KBAN, the first proxy agent PA1 of the first computer unit C1 forms a get request, i.e. a fetch message ABN. To this end, a fourteenth means 117 is provided for forming and encoding the fetch message ABN according to the encoding format of the SNMPv1 protocol, the cryptographically processed reply message KBAN being requested therewith from the second computer unit C2. Further, the encoded fetch message ABN is sent from the first computer unit C1 to the second computer unit C2.

In an eighteenth step 118, the fetch message ABN, i.e. the get request in this case, is received in the second proxy agent PA2 and, in conformity with the standard, the standard get response, which contains the cryptographically processed reply message KBAN in this case, is sent to the first proxy agent PA1. To this end, a fifteenth means 118 is provided in the second computer unit C2 for receiving the fetch message ABN and for encoding the cryptographically processed reply message KBAN requested in the fetch message ABN according to the encoding format of the SNMPv1 protocol, i.e. for encoding the requested get response.

The encoded, cryptographically processed reply message is transmitted from the second proxy agent PA2 to the first proxy agent PA1.

In a further step 119, the encoded, cryptographically processed reply message contained in the standard-conforming get response is received in the first proxy agent PA1. A sixteenth means 119 for receiving the get response is provided for this purpose in the first computer unit C1.

In a further step 120, the get request is decoded, i.e. de-encapsulated, and the get response originally formed by the agent AG of the second computer unit C2 is sent to the manager application MA of the first computer unit C1. A seventeenth means 120 for decoding the get response and for sending the original get response contained in the get response [sic] that contains the requested information is provided for the manager application MA.

In a last step 121, the get response is received by the manager application MA and the requested value is interpreted and stored. An eighteenth means 121 for receiving and evaluating management information is provided for this purpose in the manager application MA.

What is achieved in this way is that a cryptographic securing of the communication becomes possible without great added outlay and without having to modify the method of the SNMPv1 protocol.

Get-Net-Request

For a get next request, which is likewise provided within the framework of the SNMPv1 protocol, the method is implemented in the same way as described for the get request, merely with a modified, correspondingly adapted object identifier for the requested value of the respective managed object.

Set-Request

Figure 2 shows the method for a set request as encoded, digital message CN. For simpler explanation, only the method is described below; the means are correspondingly fashioned such that the individual method steps can be implemented with the computer units C1, C2.

In a first step 201, the set request, i.e. the digital message, is encoded.

In a second step 202, the manager MA of the first computer unit sends the set request, i.e. the encoded message CN, to the first proxy agent PA1.

In a third step 203, the encoded message CN is received by the first proxy agent PA1.

In a fourth step 204, a cryptographic process is applied to the encoded message CN. The result of the cryptographic processing is a cryptographically processed message KBN.

In a fifth step 205, the cryptographically processed message KBN is again encoded upon employment of the encoding format of the SNMPv1 protocol to form an encoded, cryptographically processed message CKN. A set request is again employed for this purpose.

The set request is sent from the first proxy agent PA1 to the second proxy agent PA2 (step 206).

In a seventh step 207, the second proxy agent PA2 receives the set request.

As a reaction to the reception of the set request, the second proxy agent PA2 sends a get response in conformity with the standard that contains the error status as confirmation (step 208).

In a further step 209, the encoded, cryptographically processed message is decoded, i.e. “unpacked”. The result is the decoded, cryptographically processed message DKN.

In a tenth step 210, the cryptographic method respectively inverse relative to the cryptographic method employed is applied to the cryptographically processed message DKN. Further, the inversely cryptographically processed message IKN, i.e. the original set request, is sent from the second proxy agent PA2 to the agent AG of the second computer unit C2.

In an eleventh step 211, the agent AG receives decoded, cryptographically processed message and, in a further step 212, the action indicated in the set request is implemented.

As reaction, the agent AG of the second computer unit CU sends the reply message AN in the form of a get response to the second proxy agent PA2 in conformity with the standard (step 213).

In a fourteenth step 214, the second proxy agent PA2 receives the reply message AN.

In a fifteenth step 215, at least one prescribable cryptographic method is again applied to the reply message AN.

The further method steps 216, 217, 218, 219, 220 as well as 221 correspond to the method steps 116, 117, 118, 119, 120 as well as to 121 described in conjunction with a get request method.

The security MIB contains entries that employ the usual syntax for describing managed objects in their structure. Entries in the security MIB are assigned unambiguous object identifiers that are employed for the unambiguous identification of the entries in the security MIB. The object identifiers are registered in the global SNMP-MIB. What is thus achieved is that the purpose and the syntax of the respective managed object is known. The various entries of the security MIB can, for example, contain either digitally signed, integrity-protected or encrypted management information. Of course, arbitrary combinations of the above-described mechanisms can be entered in the security MIB and, thus, can be taken into consideration in the framework of the method.

A possible exemplary syntax in AS1.1 (abstract syntax notation one) of such a security MIB is presented below.

The syntax of a secure, encapsulated managed object is OCTET STRING. The structure of such an encapsulated managed object is as follows:

```
SecureMO ::=
        SEQUENCE {
              PlainHeader,
              EncapsulatedData
        }
PlainHeader ::=
        SEQUENCE {
              SecurityAssociationID,
              UsedAlgorithms,
              AlgorithmParameters
        }
EncapsulatedData ::= OCTET STRING
        -- signed, encrypted, or integrity protected
        -- ASN.1-encoded data
SecurityAssociationID ::= OBJECT IDENTIFIER
UsedAlgorithms ::= INTEGER (0..7)
        -- value 0 stands for "no security"
        — value 1 stands for "signed"
        -- value 2 stands for "integrity protected"
        -- value 3 stands for "signed" and "integrity protected"
```

-- value 4 stands for “encrypted”

-- value 5 stands for “signed” and “encrypted”

-- value 6 stands for “integrity protected” and “encrypted”

-- value 7 stands for “signed”, “integrity protected” and “encrypted”

AlgorithmParameters ::=

-- necessary parameters for the particular

-- algorithms in use

The value of the parameter UsedAlgorithms is formed according to the following strategy. It can be represented as bit string having the length of 3 bits, whereby the bit of least significance indicates the employment of digital signature (“signed”); the bit having the second lowest significance indicates, for example, whether mechanisms for the protection of the data integrity are provided (“integrity protected”), and the bit having the highest significance describes whether the data were encrypted.

The result of every cryptographic processing of a message can thus be described as bit string having the length 3. The cryptographically processed message is encoded as OCTET STRING. When it is composed of a plurality of bits not divisible by 8, then, however, it can be expanded into an OCTET STRING by employing what is referred to as padding, i.e. filling bits in without semantic significance.

This situation is shown by way of example in a flowchart in Figure 3.

An SNMPv1 request SR is encoded 301 into ASN.1 (encoding rules, syntax definition, ER) according to the rules for encoding of the respective network protocol. The encoded SNMP request CSR, i.e. the encoded message CN, is subjected to the respective cryptographic process in a second step 302. For example, cryptographic keys, parameters for indicating the algorithm employed, as well as additional information, general cryptographic information VI, for the implementation of the respective cryptographic method are thereby employed.

The deriving bit string BS is converted into an OCTET STRING OS by, for example, filling with filler bits in a step 303, for example upon employment of padding PA.

The abstract procedure for the inverse cryptographic processing is correspondingly inversely implemented.

It is advantageous to apply existing functions for the protection of the communication in the framework of SNMPv1 where it is possible and to strengthen these security functions with further cryptographic processes as necessary.

Thus, it is advantageous to employ the concept of community strings in SNMPv1 in the framework of this method as well. In the framework of the concept of a community, groups are defined and access rights for the respective members of the group are allocated to the individual groups. A community and the access rights allocated to the community are part of a configuration of an SNMPv1 agent. It is advantageous to respectively associate communities with specific security mechanisms. Thus, for example, it is possible to assign different cryptographic algorithms, cryptographic keys and corresponding parameters that are respectively employed in the framework of the cryptographic method to members of the community in a community.

Standard-conforming object identifiers are preferably employed as particulars that are to be employed in the cryptographic processes.

In the security configuration, object identifiers are preferably applied to stored cryptographic keys instead of cryptographic keys, these being referred to below as key identifiers. The respective key material is protected better as a result of this procedure.

Further, the respective key material can thereby be more highly protected in that, for example, the data files wherein the cryptographic keys are maintained are encrypted or specific hardware units are provided for the protection of the cryptographic keys, for example chip cards.

The realization details to be respectively employed derive from the security policy, which can vary greatly in conformity with the application.

Authentification of the Data Source

In order to achieve the security service of authentification of the source data, the following information can, for example, be provided in the cryptographically processed message (see Figure 4).

The SNMPv1 request, i.e. the encoded message CN, is encapsulated with the following header or, respectively, trailer information by the cryptographic processing, as a result whereof the cryptographically processed message KBN arises.

An authentification header AH contains a key identifier KID with which the cryptographic key to be respectively employed is indicated via an object identifier, an algorithm identifier AID with which the respective cryptographic algorithm to be applied for authentification is indicated, algorithm parameters AP with which the parameters that are to be employed within the framework of the authentification are indicated, a time stamp TS as well as a random number RN.

Further, a digital signature DS is provided as trailer information TI. For example, the asymmetrical RSA method can be employed as algorithm for the authentification.

Access Control for Management Information

The SNMPv1 access control is based on two mechanisms. First, an access control value is allocated to each managed object in an MIB, this comprising one of the three following values:

- read only,
- read-write,
- write only,
- not accessible.

Second, what is referred to as an MIB viewed together with the respective access rights is allocated to each community in the SNMPv1 agent configuration. An

MIB view contains a prescribable plurality of object identifiers that indicate the respective sub-trees or what are referred to as leaves of the SNMP registration tree.

The respective access rights comprise one of the following values:

- read only,
- write only,
- read-write,
- none.

Security of the Data Integrity of an SNMP Request

A mechanism for the cryptographic protection of the data integrity is utilized for securing the data integrity. Data integrity checksums are formed over the entire SNMPv1 request or over a part thereof for this purpose. This can ensue, for example, with the DES in what is referred to as the cipher block chaining mode (CBC mode). The employment of a 64 bit long initialization value is required for this specific mechanism, this having to be known to every party of the respective security group. The initialization value is part of the algorithm parameter AP that is employed in the header information HI of the cryptographically processed message KBN (see Figure 5). Further, the header information HI comprises a key identifier KID as well as an algorithm identifier AID whose functionality is the same as in the authentification.

Further, an integrity checksum ICV is provided in a trailer information TI.

Encryption of SNMPv1 Requests

Confidentiality of the transmitted SNMPv1 data can ensue in a way similar to the protection of the data integrity. For example, the DES method in the CBC mode can again be employed for the encryption. In this case, an initialization value is again required as algorithm parameter AP and a header information HI of the cryptographically processed message KBN is required (see Figure 6).

A key identifier KID as well as an algorithm identifier AID having the above-described functionality are again provided in the header information HI.

Further, mechanisms for logging the communication as well as for outputting an alarm when attempted attacks are found can be provided.

The method and the computer system can be very advantageously employed within the framework of a scenario wherein a vendor of a communication network makes bandwidth of the communication network available to a service provider who makes additional services available to third parties that do not provide the communication network in and of itself. In this context, the method as well as the computer system can advantageously serve, for example, for controlling or for accounting for the resources made available by the vendor of the overall communication network. In this case, the manager will be realized on a computer of the vendor of the overall communication network and an agent will be realized at the respective provider of additional services.

It is provided in one version of the above described exemplary embodiment to directly encode the reply message without waiting for a fetch message and to send it to the first computer unit. The following steps are thus not required in the second computer unit:

- the encoding of a fetch message according to the encoding format of the network protocol in the first computer unit, with which the cryptographically processed reply message is requested from the second computer unit;
- the transmission of the fetch message from the first computer unit to the second compute unit; as well
- the reception of the fetch message.

The analogous case applies to the computer system.

Clearly, the method can be described such that a cryptographic process is applied to the standard-conforming network protocol, for example the SNMPv1 protocol, being applied to the respective SNMP request or CMIP request as well, a cryptographic protection of the SNMP request or, respectively, the CMIP request being achieved with this. In order, however, to enable the employment of standard-conforming SNMP methods, the cryptographically processed message is again encoded with the respective encoding format of the network protocol. This corresponds to a “double” application of the respective network protocol to the message to be encoded.

Patent Claims

1. Method for encoding a digital message upon employment of an encoding format of a network protocol,

- whereby the message is encoded to form an encoded message upon employment of the encoding format of the network protocol;

- whereby the encoded message is subjected to at least one cryptographic process; and

- whereby the cryptographically processed message is encoded upon employment of the encoding format of the network protocol.

2. Method for decoding a digital message that is present in an encoding format of a network protocol,

- whereby the message is decoded according to the encoding format of the network protocol;

- whereby the decoded, cryptographically processed message is subjected to a cryptographic process inverse relative to the at least one cryptographic process; and

- whereby the inversely cryptographically processed message is decoded according to the encoding format of the network protocol.

3. Method for encoding a digital message, for transmission of the message from a first computer unit to a second computer unit and for decoding the message,

- whereby the following steps are implemented in the first computer unit:

-- the message is encoded into an encoded message upon employment of an encoding format of a network protocol;

-- the encoded message is [...] to at least one cryptographic process;

-- the cryptographically processed message is encoded upon employment of the encoding format of the network protocol,

- whereby the encoded, cryptographically processed message is transmitted from the first computer unit to the second computer unit,

- whereby the following steps are implemented in the second computer unit:

-- the received message is decoded according to the encoding format of the network protocol;

- the decoded, cryptographically processed message is subjected to a cryptographic process inverse relative to at least one cryptographic process; and

- the inversely cryptographically processed message is decoded into the digital message according to the encoding format of the network protocol.

4. Method according to claim 3,

- whereby the digital message contains a request for implementation of a prescribable action;

- whereby the requested action is implemented in the second computer unit; and

- whereby the result of the action in the second computer unit is sent to the first computer unit in a reply message.

5. Method according to claim 3

- whereby the digital message contains a request for implementation of a prescribable action;

- whereby the requested action is implemented in the second computer unit;

- whereby a reply message that contains a result of the action is formed in the second computer unit;

- whereby the reply message is encoded in the second computer unit according to the encoding format of the network protocol;

- whereby the reply message is subjected to at least one cryptographic process in the second computer unit;

- whereby the cryptographically processed reply message is stored in the second computer unit;

- whereby a fetch message is encoded in the first computer unit according to the encoding format of the network protocol, the cryptographically processed reply message being requested from the second computer unit therewith;

- whereby the fetch message is transmitted from the first computer unit to the second computer unit;
- whereby the fetch message is received by the second computer unit;
- whereby the cryptographically processed reply message is encoded according to the encoding format of the network protocol; and
- whereby the encoded, cryptographically processed reply message is transmitted from the second computer unit to the first computer.

6. Method according to claim 3,

- whereby the digital message contains a request for implementation of a prescribable action;
- whereby the requested action is implemented in the second computer unit;
- whereby a reply message that contains a result of the action is formed in the second computer unit;
- whereby the reply message is encoded in the second computer unit according to the encoding format of the network protocol;
- whereby the reply message is subjected to at least one cryptographic process in the second computer unit;
- whereby the cryptographically processed reply message is encoded according to the encoding format of the network protocol; and
- whereby the encoded, cryptographically processed reply message is transmitted from the second computer unit to the first computer unit.

7. Method according to one of the claims 2 through 6, whereby the cryptographically processed reply message is stored in a management information base (MIB) in the second computer unit.

8. Method according to one of the claims 1 through 4, whereby the simple network management protocol version 1 (SNMPv1) is employed as network protocol.

9. Method according to claim 8,

- whereby a set request is formed in the first computer unit in the encoding of the cryptographically processed message; and

- whereby the set request is transmitted from the first computer unit to the second computer unit.

10. Method according to claim 8 or 9,

- whereby a get request is employed as fetch message;

- whereby a get response is formed in the encoding of the requested, cryptographically processed reply message.

11. Method according to one of the claims 4 through 10, whereby an information query and/or an information indication of the second computer unit is transmitted as action.

12. Apparatus comprising at least one computer unit that is configured such that the method according to one of the claims 1 through 11 can be implemented.

13. Apparatus for encoding a digital message upon employment of an encoding format of a network protocol, comprising at least the following components:

- a first means for encoding the digital message upon employment of the encoding format of the network protocol to form an encoded message;

- a second means for the cryptographic processing of the encoded message;

- a third means for encoding the cryptographically processed message upon employment of the encoding format of the network protocol.

14. Apparatus for decoding a digital message that is present in an encoding format of a network protocol, comprising at least the following components:

-- a fifth means for receiving the encoded, cryptographically processed message from the first computer unit;

-- a sixth means for decoding the received message according to the encoding format of the network protocol;

-- a seventh means for the inverse cryptographic processing of the decoded, cryptographically processed message; and

-- an eighth means for the decoding of the inversely cryptographically processed message according to the encoding format of the network protocol.

15. Apparatus for encoding a digital message, for transmission of the message from a first computer unit to a second computer unit and for decoding the message,

- whereby a first computer unit is provided that comprises at least the following components:

-- a first means for encoding the digital message upon employment of an encoding format of a network protocol to form an encoded message,

-- a second means for the cryptographic processing of the encoded message,

-- a third means for encoding the cryptographically processed message upon employment of the encoding format of the network protocol,

-- a fourth means for sending the encoded cryptographically processed message from the first computer unit to the second computer unit;

- whereby a second computer unit is provided that comprises at least the following components:

-- a fifth means for receiving the encoded, cryptographically processed message from the first computer unit,

-- a sixth means for decoding the received message according to the encoding format of the network protocol,

-- a seventh means for the inverse cryptographic processing of the decoded, cryptographically processed message, and

-- an eighth means for decoding the inversely cryptographically processed message according to the encoding format of the network protocol.

16. Apparatus according to claim 13 or 15, whereby the first means is provided as third means.

17. Apparatus according to claim 14 or 15, whereby the sixth means is provided as eighth means.

18. Apparatus according to one of the claims 15 through 17

- whereby the digital message contains a request for implementation of a prescribable action;

- whereby a ninth means for the implementation of the requested action is provided in the second computer unit; and

- whereby a tenth means is provided in the second computer unit for sending the result of the action to the first computer unit.

19. Apparatus according to one of the claims 15 through 18

- whereby the digital message contains a request for implementation of a prescribable action;

- whereby a ninth means is provided in the second computer unit for the implementation of the requested action;

- whereby an eleventh means is provided in the second computer unit for forming a reply message that contains a result of the action;

- whereby a twelfth means is provided in the second computer unit for encoding the reply message according to the encoding format of the network protocol;

- whereby a thirteenth means is provided in the second computer unit for processing the reply message with at least one cryptographic process;

- whereby a fourteenth means is provided in the second computer unit for storing the cryptographically processed reply message;

- whereby a fifteenth means is provided in the first computer unit for forming and encoding a fetch message according to the encoding format of the network protocol, with which the cryptographically processed reply message is requested from the second computer unit;

- whereby a sixteenth means is provided in the first computer unit for sending the fetch message from the first computer unit to the second computer unit;

- whereby a seventeenth means is provided in the second computer unit for receiving the fetch message;

- whereby an eighteenth means is provided in the second computer unit for encoding the cryptographically processed reply message requested in the fetch message according to the encoding format of the network protocol; and

- whereby a nineteenth means is provided in the second computer unit for sending the encoded, cryptographically processed reply message from the second computer unit to the first computer unit.

20. Apparatus according to one of the claims 15 through 18

- whereby the digital message contains a request for implementation of a prescribable action;

- whereby a ninth means is provided in the second computer unit for the implementation of the requested action;

- whereby an eleventh means is provided in the second compute unit for formation of a reply message that contains a result of the action;

- whereby a twleveth means is provided in the second computer unit for encoding the reply message according to the encoding format of the network protocol;

- whereby a thirteenth means is provided in the second computer unit for processing the reply message with at least one cryptographic process;

- whereby an eighteenth means is provided in the computer unit for encoding the cryptographically processed reply message according to the encoding format of the network protocol; and

- whereby a nineteenth means is provided in the second computer unit for sending the encoded, cryptographically processed reply message from the second computer unit to the first compute unit.

21. Apparatus according to claim 19 or 20, whereby the fourteenth means is fashioned such that the cryptographically processed reply message is stored in a management information base (MIB).

22. Apparatus according to one of the claims 13 through 21 that is fashioned such that the simple network management protocol version 1 (SNMPv1) is employed as network protocol.

23. Apparatus according to claim 13 or 15,

- that is fashioned such that the simple network management protocol version 1 (SNMPv1) is employed as network protocol; and

- whereby the third means for encoding the cryptographically processed message is fashioned such that a set request is formed in the encoding of the cryptographically processed message.

24. Apparatus according to claim 22

- whereby the fifteenth means for forming and encoding the fetch message is fashioned such that a get request is formed;

- whereby the eighteenth means for encoding the cryptographically processed reply message requested in the fetch message is fashioned such that a get response is formed.

25. Apparatus according to one of the claims 15 through 24, whereby an information query and/or an information particular of the second computer unit is provided as action.

26. Apparatus according one of the claims 12 through 25, whereby the second means, a third means and the fourth means are fashioned together as a first proxy agent; and/or

whereby the fifth means, the sixth means and the seventh means are fashioned together as a second proxy agent.

27. Communication system having a manager of a communication network and an intermediate manager of a communication network that employs the communication network and offers further services that proceed beyond the services offered by the communication network to customers, comprising a computer system according to one of the claims 13 through 26.

Abstract

Method and Computer System for Encoding a digital message, for transmission of the message from a first computer unit to a second computer unit, and for decoding the message

A method is presented wherein, for a network protocol, for example for the SNMPv1, a message is encoded (101) in the first computer unit (C1) upon employment of the encoding format of the network protocol, being encoded to form an encoded message (CN). The encoded message (CN) is subjected (104) to a cryptographic process. The cryptographically processed message (KBN) thereby formed is again encoded (105) upon employment of the encoding format of the network protocol. The cryptographically processed message (CKN) encoded in this way is transmitted from the first computer unit (C1) to the second computer unit (C2). In the second computer unit (C2), the received message is decoded (109) according to the encoding format of the network protocol, and an inverse cryptographic process (110) is applied to the decoded message (DKN). The inversely cryptographically processed message (IKN) is again decoded according to the encoding format of the network protocol.

Figure 1

FIG 1A

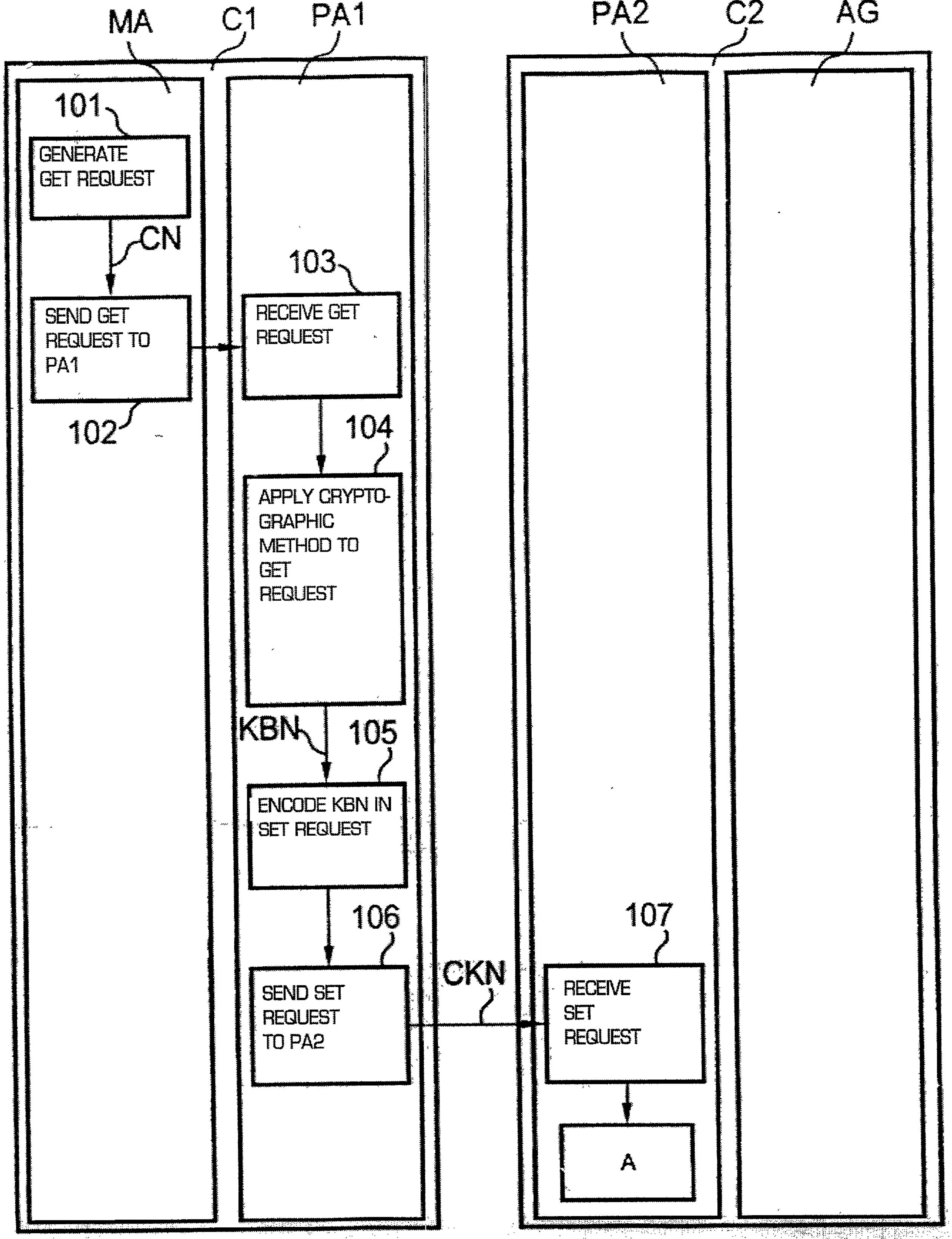

MA
C1
PA1
PA2
C2
AG
101
GENERATE GET REQUEST
CN
SEND GET REQUEST TO PA1
102
103
RECEIVE GET REQUEST
104
APPLY CRYPTO-GRAPHIC METHOD TO GET REQUEST
KBN
105
ENCODE KBN IN SET REQUEST
106
SEND SET REQUEST TO PA2
CKN
107
RECEIVE SET REQUEST
A

FIG 1b

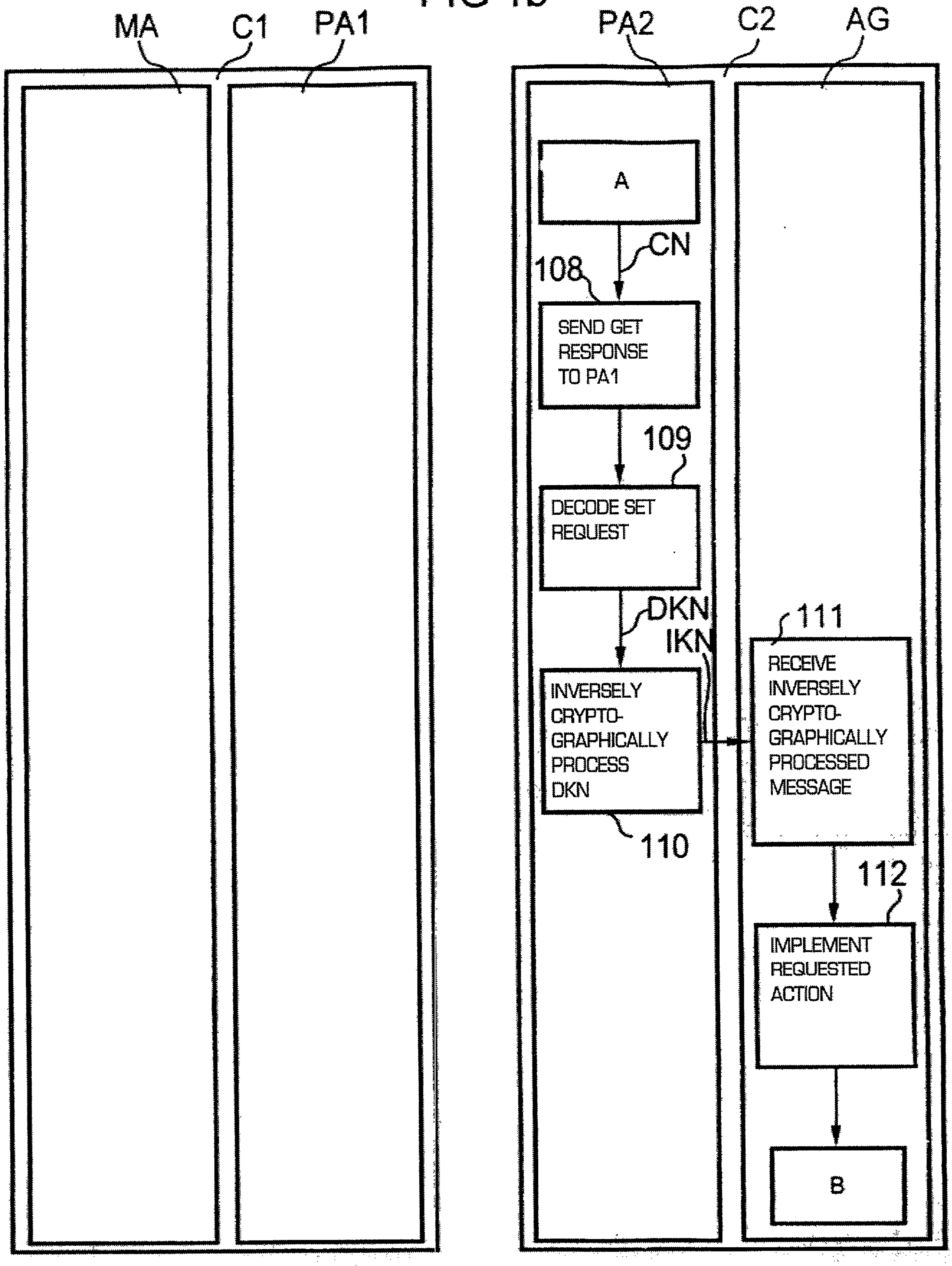
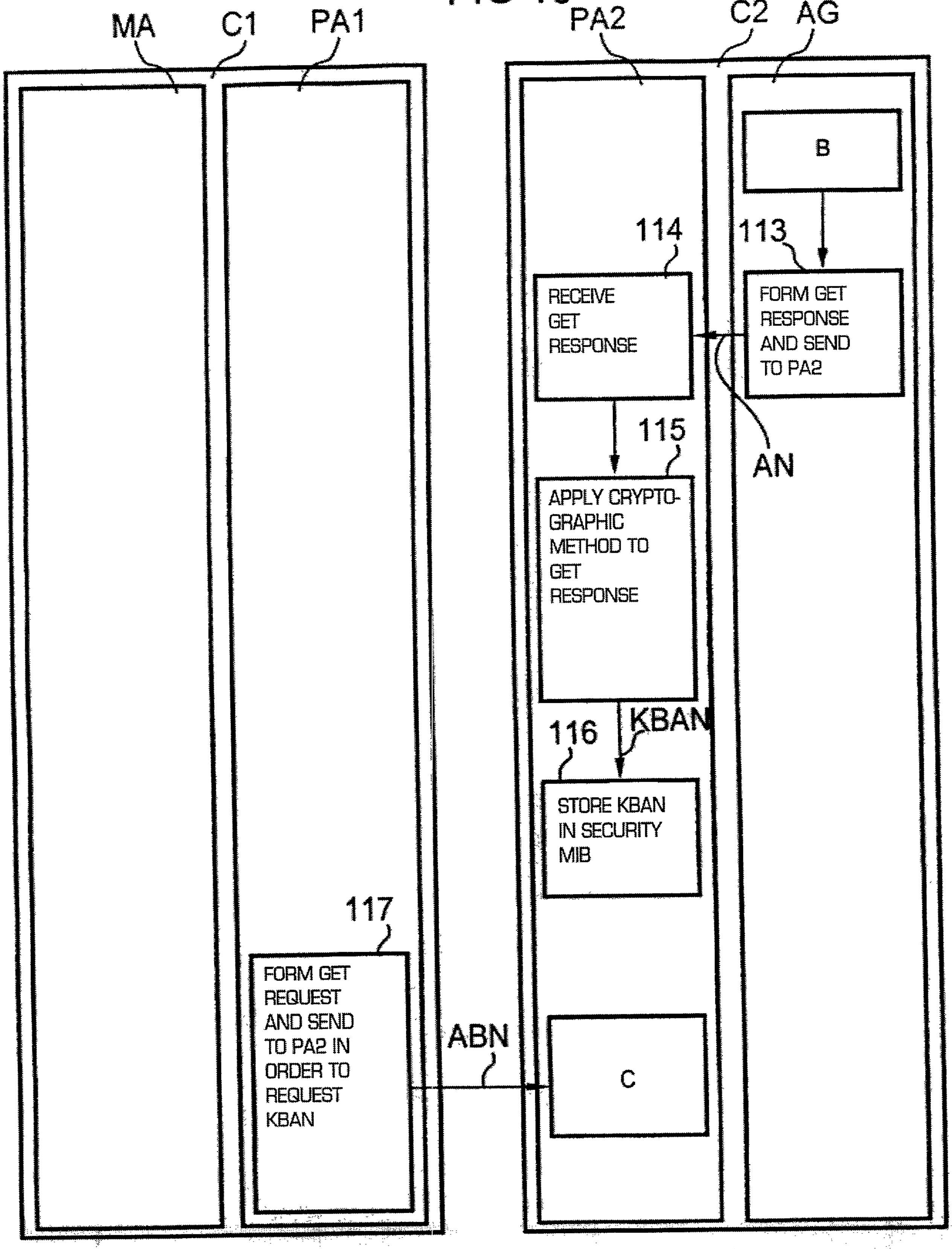

MA
C1
PA1
PA2
C2
AG
A
CN
108
SEND GET RESPONSE TO PA1
109
DECODE SET REQUEST
DKN
IKN
INVERSELY CRYPTO-GRAPHICALLY PROCESS DKN
110
111
RECEIVE INVERSELY CRYPTO-GRAPHICALLY PROCESSED MESSAGE
112
IMPLEMENT REQUESTED ACTION
B

FIG 1c


MA
C1
PA1
PA2
C2
AG
B
114
113
RECEIVE GET RESPONSE
FORM GET RESPONSE AND SEND TO PA2
115
AN
APPLY CRYPTOGRAPHIC METHOD TO GET RESPONSE
116
KBAN
STORE KBAN IN SECURITY MIB
117
FORM GET REQUEST AND SEND TO PA2 IN ORDER TO REQUEST KBAN
ABN
C

09/446425

FIG 1d

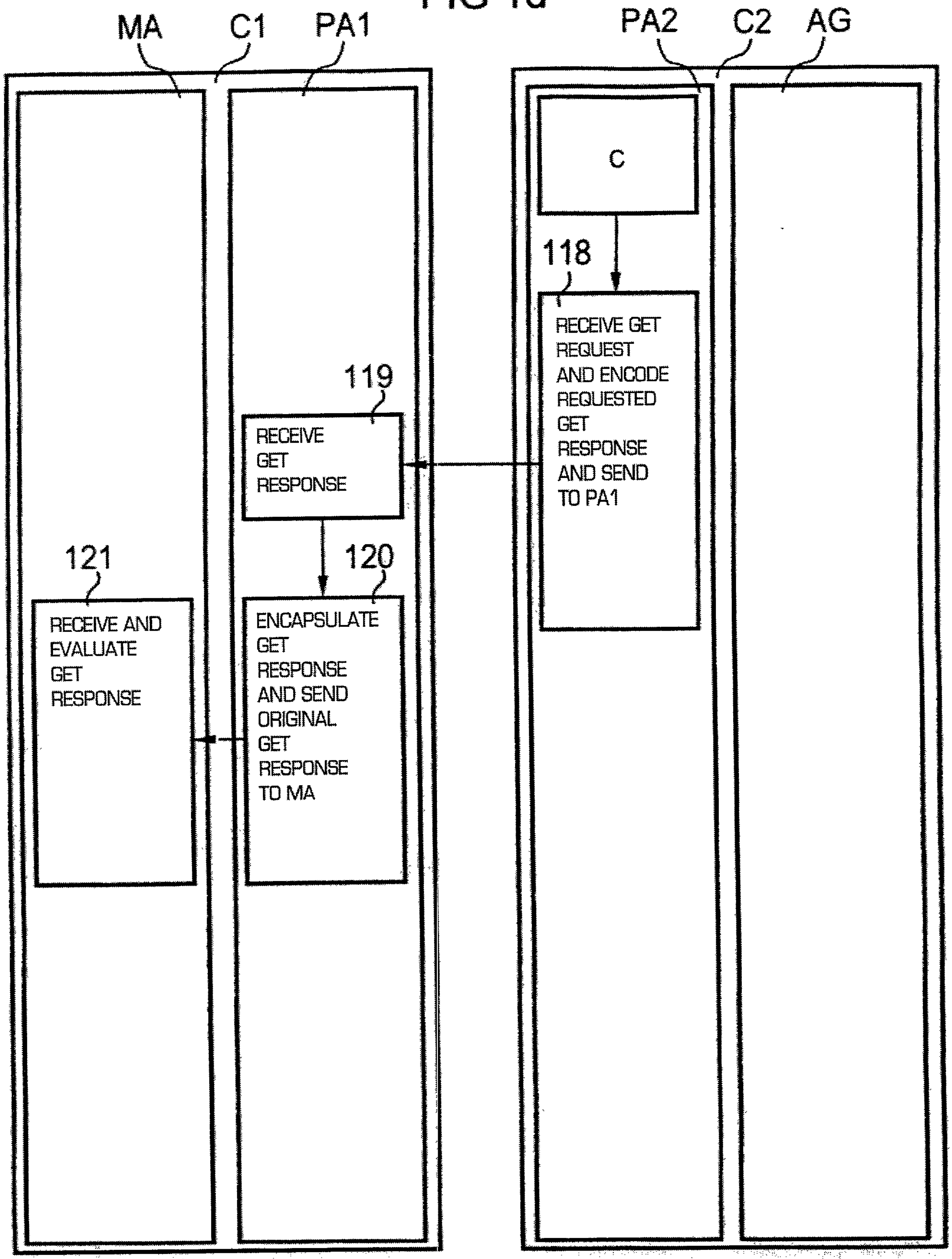

MA
C1
PA1
PA2
C2
AG
C
118
RECEIVE GET REQUEST AND ENCODE REQUESTED GET RESPONSE AND SEND TO PA1
119
RECEIVE GET RESPONSE
120
ENCAPSULATE GET RESPONSE AND SEND ORIGINAL GET RESPONSE TO MA
121
RECEIVE AND EVALUATE GET RESPONSE

FIG 2A

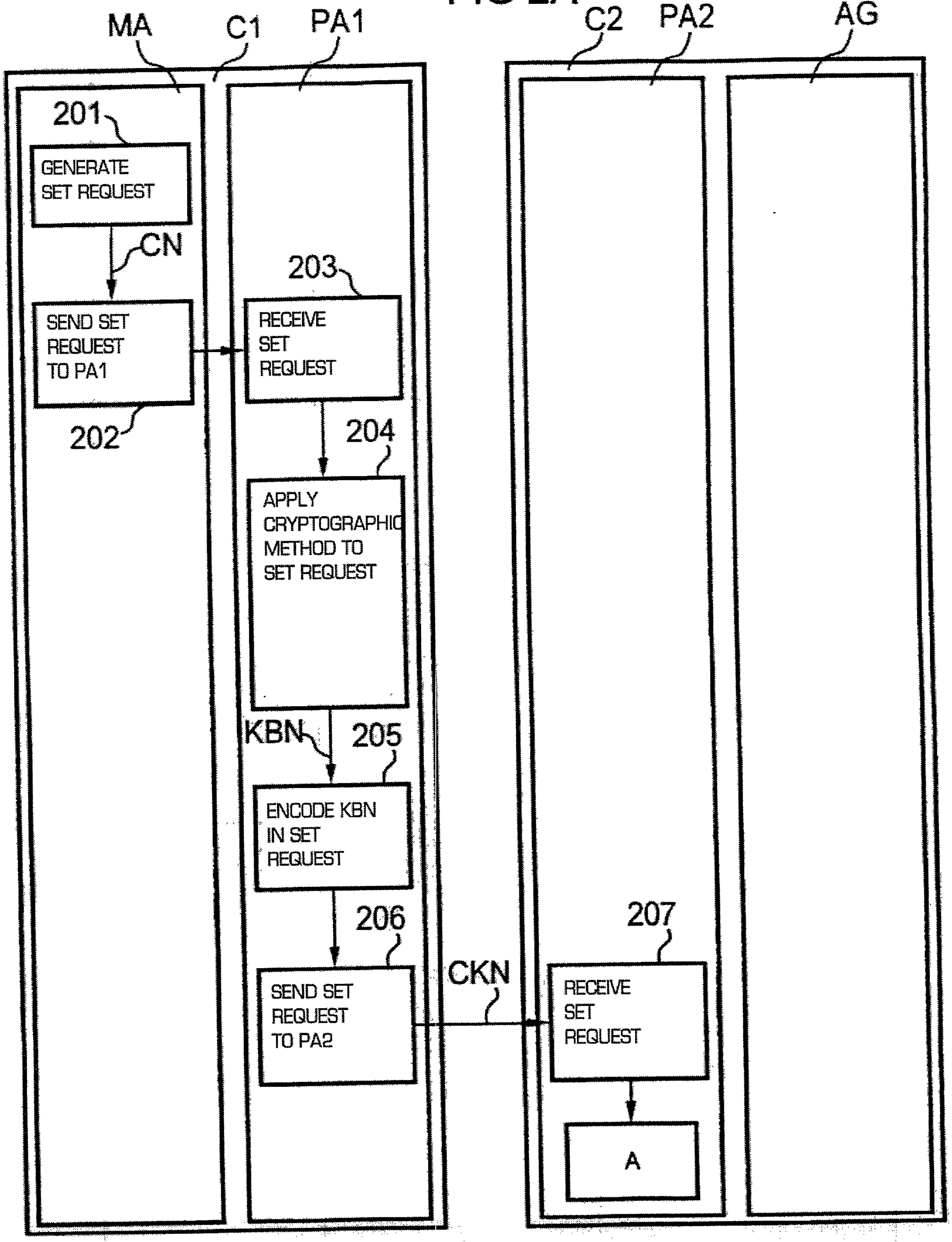

MA
C1
PA1
C2
PA2
AG
201
GENERATE SET REQUEST
CN
202
SEND SET REQUEST TO PA1
203
RECEIVE SET REQUEST
204
APPLY CRYPTOGRAPHIC METHOD TO SET REQUEST
KBN
205
ENCODE KBN IN SET REQUEST
206
SEND SET REQUEST TO PA2
CKN
207
RECEIVE SET REQUEST
A

FIG 2B

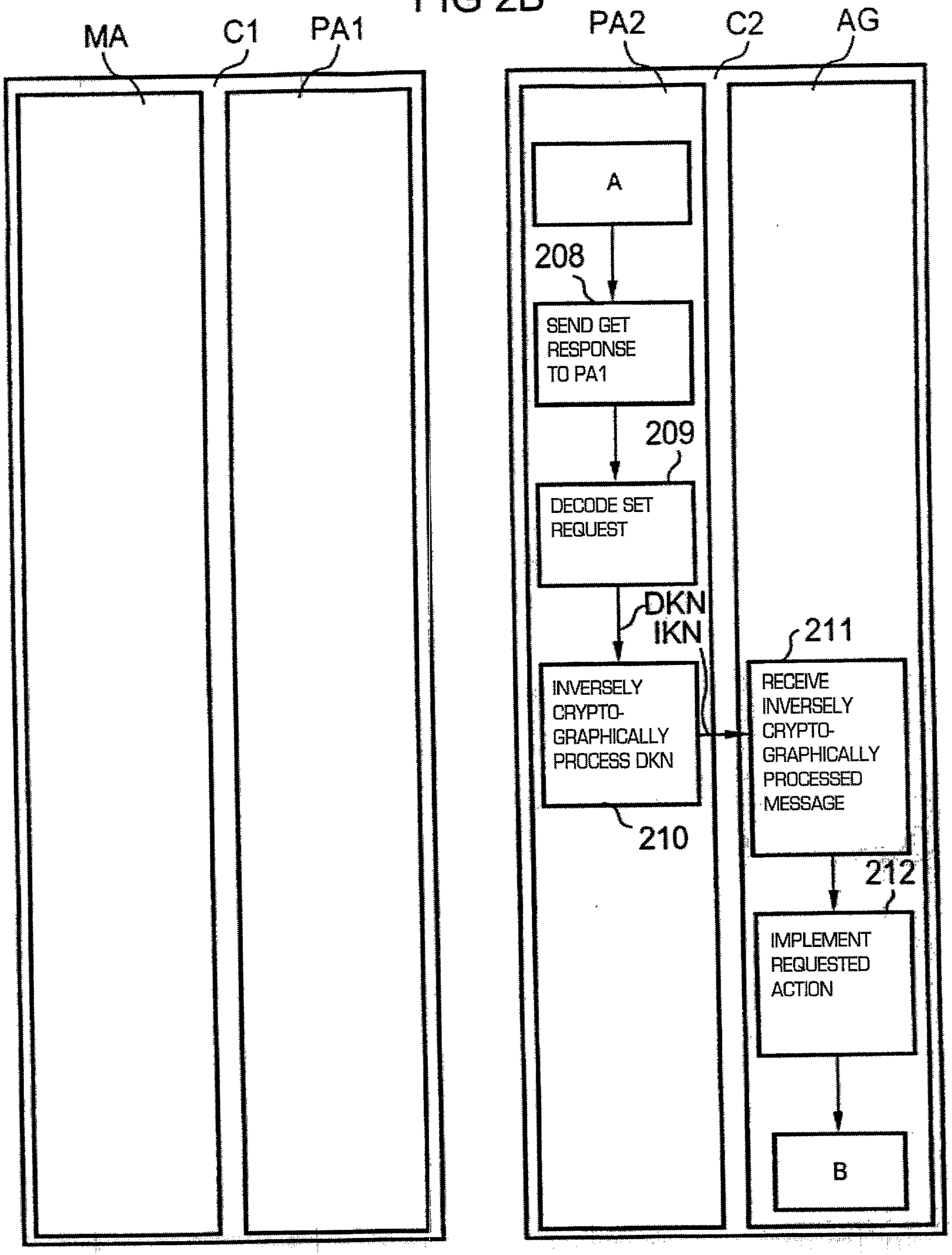

MA
C1
PA1
PA2
C2
AG
A
208
SEND GET RESPONSE TO PA1
209
DECODE SET REQUEST
DKN
IKN
INVERSELY CRYPTO-GRAPHICALLY PROCESS DKN
210
211
RECEIVE INVERSELY CRYPTO-GRAPHICALLY PROCESSED MESSAGE
212
IMPLEMENT REQUESTED ACTION
B

FIG 2C

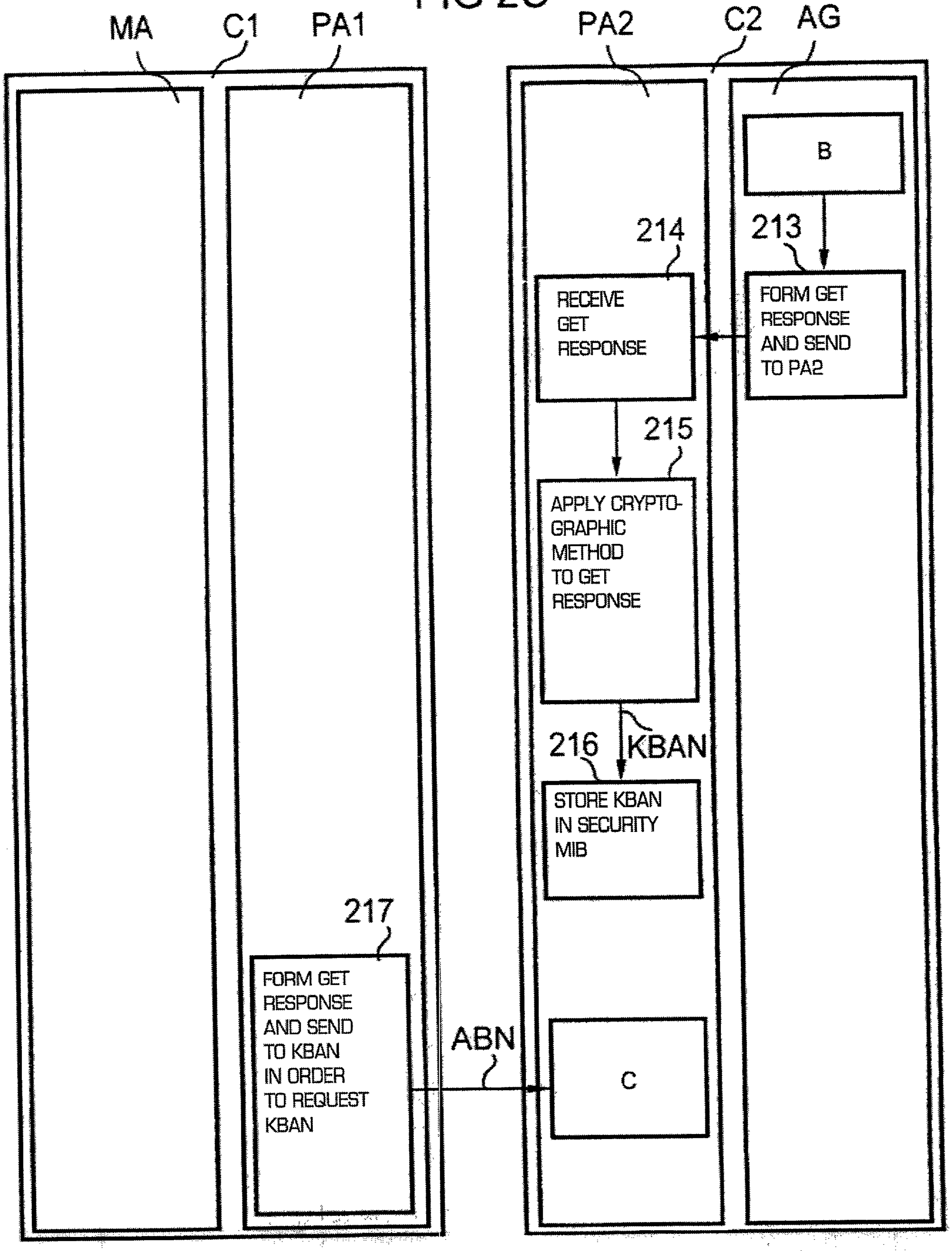

MA
C1
PA1
PA2
C2
AG
B
213
FORM GET RESPONSE AND SEND TO PA2
214
RECEIVE GET RESPONSE
215
APPLY CRYPTO-GRAPHIC METHOD TO GET RESPONSE
KBAN
216
STORE KBAN IN SECURITY MIB
217
FORM GET RESPONSE AND SEND TO KBAN IN ORDER TO REQUEST KBAN
ABN
C

FIG 2D

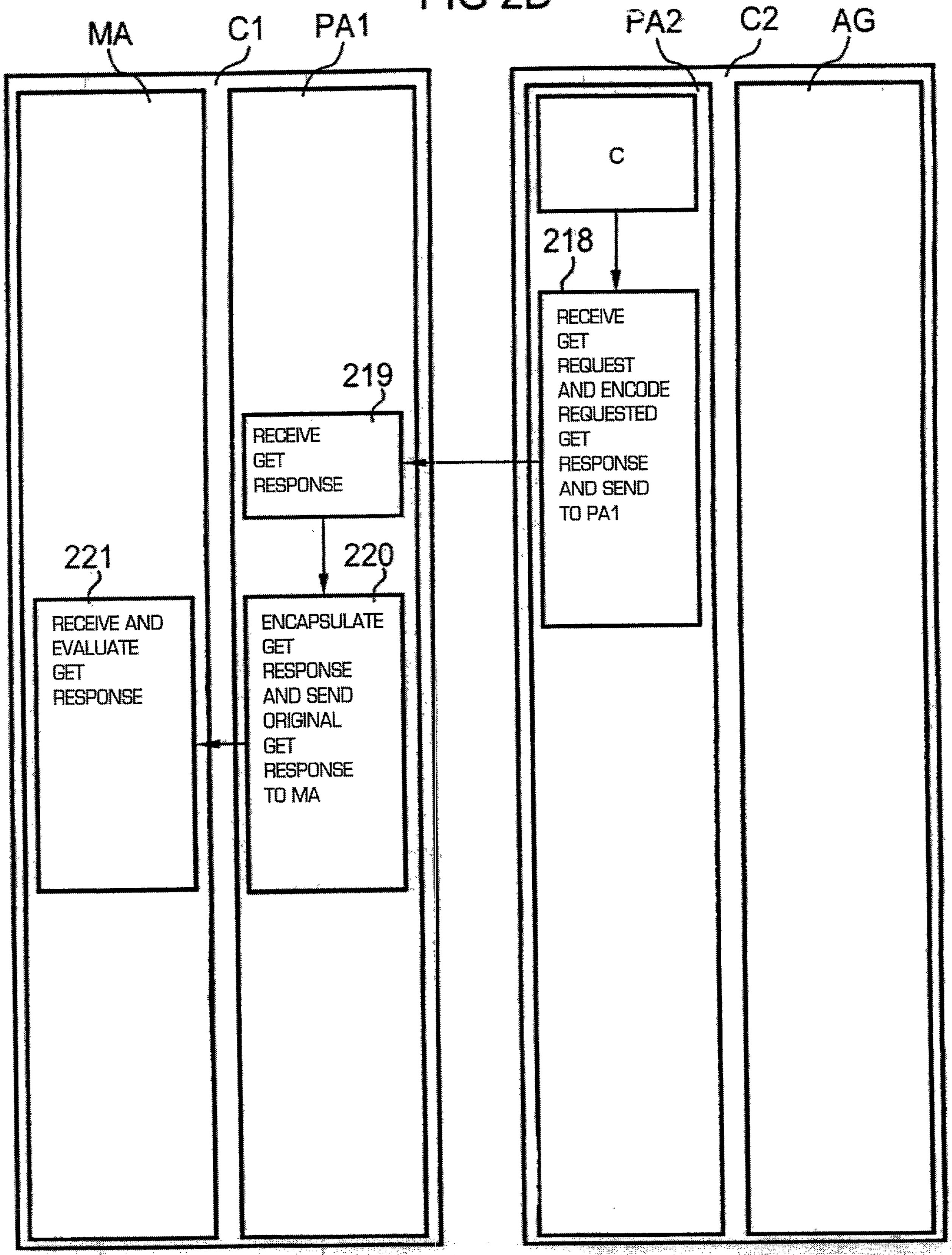

MA
C1
PA1
PA2
C2
AG
C
218
RECEIVE GET REQUEST AND ENCODE REQUESTED GET RESPONSE AND SEND TO PA1
219
RECEIVE GET RESPONSE
220
ENCAPSULATE GET RESPONSE AND SEND ORIGINAL GET RESPONSE TO MA
221
RECEIVE AND EVALUATE GET RESPONSE

FIG 3

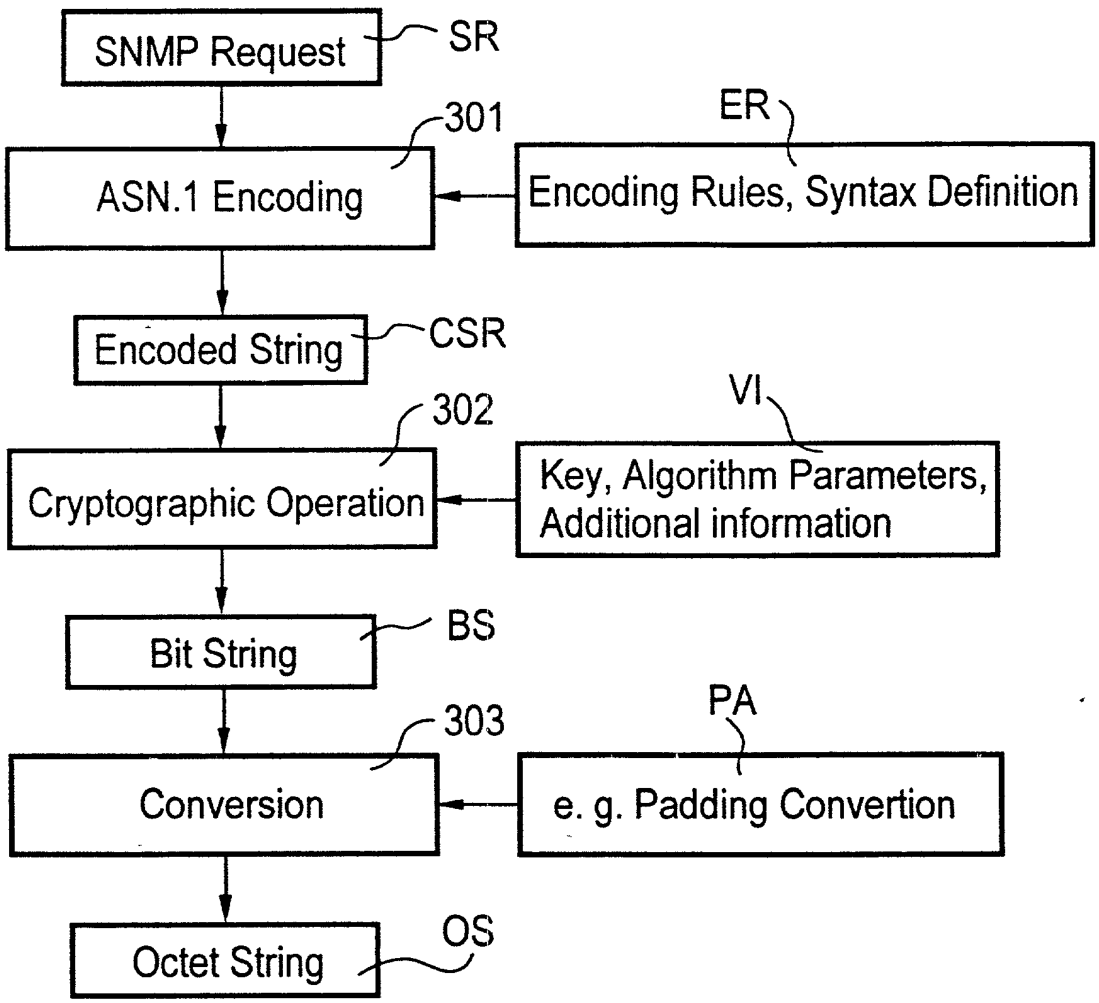

SNMP Request
SR
301
ER
ASN.1 Encoding
Encoding Rules, Syntax Definition
Encoded String
CSR
302
VI
Cryptographic Operation
Key, Algorithm Parameters, Additional information
Bit String
BS
303
PA
Conversion
e. g. Padding Convertion
Octet String
OS

FIG 4

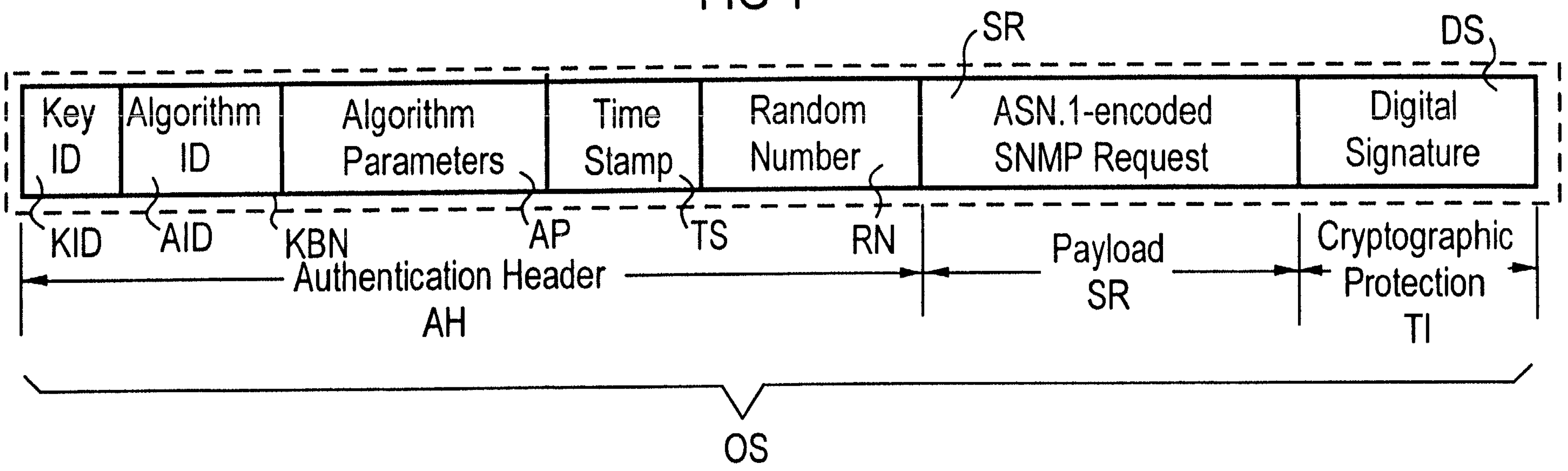

SR
DS
Key ID
Algorithm ID
Algorithm Parameters
Time Stamp
Random Number
ASN.1-encoded SNMP Request
Digital Signature
KID
AID
KBN
AP
TS
RN
Authentication Header
AH
Payload
SR
Cryptographic Protection
TI
OS

FIG 5

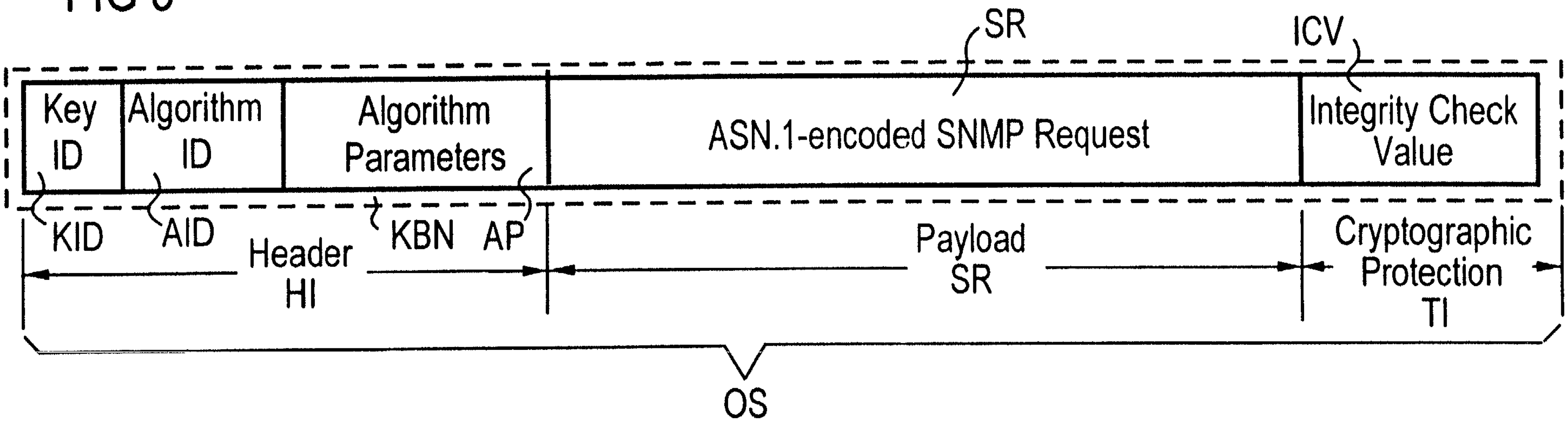
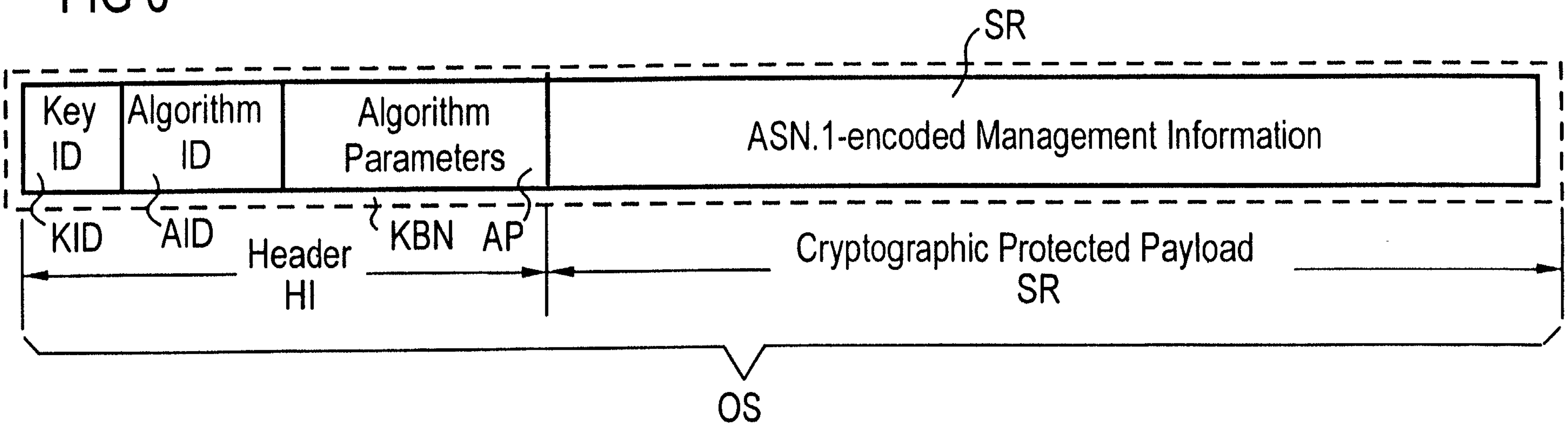

SR
ICV
Key ID
Algorithm ID
Algorithm Parameters
ASN.1-encoded SNMP Request
Integrity Check Value
KID
AID
KBN
AP
Header HI
Payload SR
Cryptographic Protection TI
OS

FIG 6


SR
Key ID
Algorithm ID
Algorithm Parameters
ASN.1-encoded Management Information
KID
AID
KBN
AP
Header HI
Cryptographic Protected Payload SR
OS

Declaration and Power of Attorney For Patent Application

Erklärung Für Patentanmeldungen Mit Vollmacht

German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Verfahren und Computersystem zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht

____
____
____
____
____
____

deren Beschreibung

(zutreffendes ankreuzen)
☒ hier beigefügt ist.
□ am ______________ als
PCT internationale Anmeldung
PCT Anmeldungsnummer ______________
eingereicht wurde und am ______________
abgeändert wurde (falls tatsächlich abgeändert).

the specification of which

(check one)
□ is attached hereto.
□ was filed on ______________ as
PCT international application
PCT Application No. ______________
and was amended on ______________
(if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign appplications
Prioritát beansprucht

Priority Claimed

197 27 267.3	Germany	26. Juni 1997	☒	□
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			□	□
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			□	□
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1 56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

And I hereby appoint

19

Messrs. John D. Simpson (Registration No. 19,842) Lewis T. Steadman (17,074), William C. Stueber (16,453), P. Phillips Connor (19,259), Dennis A. Gross (24,410), Marvin Moody (16,549), Steven H. Noll (28,982), Brett A. Valiquet (27,841), Thomas I. Ross (29,275), Kevin W. Guynn (29,927), Edward A. Lehmann (22,312), James D. Hobart (24,149), Robert M. Barrett (30,142), James Van Santen (16,584), J. Arthur Gross (13,615), Richard J. Schwarz (13,472) and Melvin A. Robinson (31,870), David R. Metzger (32,919), John R. Garrett (27,888) all members of the firm of Hill, Steadman & Simpson, A Professional Corporation.

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to: *(name and telephone number)*

312/876-0200
Ext. ______________

Postanschrift:

Send Correspondence to:

HILL, STEADMAN & SIMPSON
A Professional Corporation
85th Floor Sears Tower, Chicago, Illinois 60606

-00

Voller Name des einzigen oder ursprünglichen Erfinders: CAPELLARO, Christoph	Full name of sole or first inventor:
Unterschrift des Erfinders Datum 2.6.98	Inventor's signature Date
Wohnsitz D-82041 Oberhaching, Germany	Residence DEX
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Am Bachfeld 5	Post Office Address
D-82041 Oberhaching Bundesrepublik Deutschland	
Voller Name des zweiten Miterfinders (falls zutreffend): HOFFMANN, Gerhard	Full name of second joint inventor, if any:
Unterschrift des Erfinders Datum G. Hoffm 17.06.98	Second Inventor's signature Date
Wohnsitz D-81547 München, Germany	Residence DEX
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Gozbertstr. 8/II	Post Office Address
D-81547 München Bundesrepublik Deutschland	

2-00

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

3-00

Voller Name des dritten Miterfinders: LUKAS, Klaus	Full name of third joint inventor:
Unterschrift des Erfinders Datum Klaus Lukas 17.06.98	Inventor's signature Date
Wohnsitz D-81793 München, Germany DEX	Residence
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Niemöllerallee 6	Post Office Address
D-81793 München Bundesrepublik Deutschland	
Voller Name des vierten Miterfinders (falls zutreffend): MUNZERT, Michael	Full name of fourth joint inventor, if any:
Unterschrift des Erfinders Datum Munzert Michael 18.6.98	Inventor's signature Date
Wohnsitz D-80639 München, Germany DEX	Residence
Staatsangehörigkeit Bundesrepublik Deutschland	Citizenship
Postanschrift Renatastr. 60	Post Office Address
D-80639 München Bundesrepublik Deutschland	
Voller Name des fünften Miterfinders (falls zutreffend):	Full name of fifth joint inventor, if any:
Unterschrift des Erfinders Datum	Inventor's signature Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address
Voller Name des sechsten Miterfinders (falls zutreffend):	Full name of sixth joint inventor, if any:
Unterschrift des Erfinders Datum	Inventor's signature Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address

4-00

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

09446425 .122099